NORAD - USNORTHCOM

Detect ✯ Deter ✯ Defend

Deter ✯ Prevent ✯ Defeat ✯ Mitigate

NORAD and USNORTHCOM (N-NC) Information Technology Service Management (N2ITSM)

Peterson AFB, CO

Performance Work Statement (PWS) Core Document

11 Sept 2014

This document incorporates changes through 31 July 2014

This page left blank intentionally

TABLE OF CONTENTS

1 General

1.1 Introduction

1.1.1 North American Aerospace Defense Command (NORAD) Mission

NORAD, in close collaboration with homeland defense, security, and law enforcement partners, prevents air attacks against North America, safeguards the sovereign airspaces of the United States and Canada by responding to unknown, unwanted, and unauthorized air activity approaching and operating within these airspaces, and provides aerospace and maritime warning for North America. NORAD is a bi-national United States and Canadian organization charged with the missions of aerospace warning, aerospace control, and maritime warning. Aerospace warning includes the monitoring of man-made objects in space and the detection, validation and warning of attack against North America whether by aircraft, missiles or space vehicles. Aerospace control includes ensuring air sovereignty and air defense of the airspace of Canada and the United States. Maritime warning includes processing, assessing, and disseminating intelligence & information to warn of maritime threats or attacks against North America. To accomplish its mission, NORAD operates through three subordinate regional headquarters:

- Alaskan NORAD region
- Canadian NORAD region
- Continental NORAD region

1.1.1.1 Alaska NORAD Region (ANR)

ANR is headquartered at Elmendorf Air Force Base Alaska. ANR provides an ongoing capability to detect, validate and warn of any aircraft and cruise missile threat in its Area of Operation (AOO) that could threaten North America.

1.1.1.2 Canadian NORAD Region (CANR)

CANR is headquartered at 1 Canadian Air Division in Winnipeg, Manitoba. CANR executes a variety of tasks to defend Canadian airspace including identifying and tracking all aircraft entering Canadian airspace, exercising operational command and control of all air defense forces in CANR, and operations in support of other Government departments and agencies.

1.1.1.3 Continental NORAD Region (CONR)

CONR provides airspace surveillance and control and directs air sovereignty activities for the Continental United States (CONUS). CONR is divided into two defense sectors: the Western Defense Sector, with its headquarters located at McChord Air Force Base

Washington; and the Eastern Defense Sector, with its headquarters located at Rome, New York. Co-located with Headquarters 1st Air Force (Air Force North) at Tyndall Air Force Base, Florida, a Combined Air Operations Center coordinates CONR sector activities and executes the NORAD air sovereignty mission for the CONUS.

1.1.2 United States Northern Command (USNORTHCOM) Mission

USNORTHCOM anticipates and conducts Homeland Defense (HD) and Defense Support to Civilian Authorities (DSCA) operations within the assigned Area of Responsibility (AOR) to defend, protect and secure the United States and its interests. USNORTHCOM's AOR includes air, land and sea approaches and encompasses the CONUS, Alaska, Canada, Mexico and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico and the Straits of Florida.

USNORTHCOM's DSCA mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes. Support also includes counter-drug operations and managing the consequences of a terrorist event employing a weapon of mass destruction.

In conducting its missions, USNORTHCOM operates through established Joint Task Forces subordinate to the command as well as support from Service Components. USNORTHCOM Subordinate Commands and Service Components include:

- Joint Forces Headquarters National Capital Region
- Joint Task Force Alaska
- Joint Task Force Civil Support
- Joint Task Force North
- Army North
- Air Force North
- Navy Fleet Forces Command
- Offices of Defense Coordination, Mexico and Bahamas

1.1.2.1 Joint Forces Headquarters National Capital Region (JFHQ-NCR)

JFHQ-NCR based at Fort McNair, Washington, D.C. is responsible for land-based HD, DSCA, and incident management in the National Capital Region.

1.1.2.2 Joint Task Force Alaska (JTF-AK)

JTF-AK is headquartered at Elmendorf Air Force Base, Alaska. JTF-AK's mission is to, in coordination with other Government agencies, deter, detect, prevent and defeat threats within the Alaska Joint Operations Area (JOA) in order to protect United States territory, its citizens and interests; and as directed, conduct civil support.

1.1.2.3 Joint Task Force Civil Support (JTF-CS)

JTF-CS is headquartered at Fort Eustis in Newport News, Virginia. JTF-CS plans and integrates Department of Defense (DoD) support to the designated primary agency for domestic Chemical, Biological, Radiological, Nuclear or high-yield Explosive (CBRNE) consequence management operations.

1.1.2.4 Joint Task Force North (JTF North)

JTF North, based at Biggs Army Airfield, Fort Bliss, Texas, is the DoD organization tasked to support our nation’s federal law enforcement agencies in the interdiction of suspected transitional threats within and along the approaches to the CONUS. Transitional threats are those activities conducted by individuals or groups that involve international terrorism, narco-trafficking, alien smuggling, weapons of mass destruction and the delivery systems for such weapons that threaten the national security of the United States.

1.1.2.5 Army North (ARNORTH)

ARNORTH is located at Fort Sam Houston, Texas. ARNORTH’s mission is to conduct homeland defense, civil support operations and theater security cooperation activities. ARNORTH is responsible for developing and unifying the military response capability for CBRNE incidents.

1.1.2.6 Air Force North (AFNORTH)

AFNORTH, 1st Air Force, is headquartered at Tyndall Air Force Base, Panama City, Florida and is assigned to Air Combat Command. It has the responsibility of ensuring the air sovereignty and air defense of the CONUS. As the CONUS geographical component of NORAD (i.e., CONR), it provides airspace surveillance and controls and directs all air sovereignty activities for the CONUS.

1.1.2.7 U.S. Fleet Forces Command

U.S. Fleet Forces Command (USFF) is the Navy component of U.S. Northern Command (USNORTHCOM) to provide command and control of Department of Defense (DoD) homeland defense efforts and to coordinate defense support of civil authorities.

Located at Norfolk, Virginia, USFF's mission is to provide maritime forces prepared to conduct homeland defense, civil support operations and theater security cooperation activities when directed by USNORTHCOM.

1.1.2.8 Office of Defense Coordination

Manages all US Department of Defense Security Assistance programs both in Mexico and Bahamas; provides training opportunities for military personnel and technical support for the military.

1.1.3 N-NC/J6 Mission

The NORAD and USNORTHCOM Command Control Systems Directorate (N-NC/J6) enables information and decision superiority for the Commander, NORAD and USNORTHCOM, subordinates, and mission partners in order to optimize collaborative planning and execution in anticipation of military operations across the spectrum of missions throughout the NORAD AOO and USNORTHCOM AOR. In addition, N-NC/J6 plans and coordinates USNORTHCOM contributions to the consequence management of events affecting the communications infrastructure of the United States.

1.2 Scope

The Contractor shall provide non-personal services to manage, operate, sustain, and provide logistical and general support for the IT Services, as identified in the NORAD and USNORTHCOM IT Service Catalog, Appendix D, and service assets listed in the Hardware and Software Service Asset catalogs (Technical Library).

The Contractor is accountable for the ownership of all functions and processes identified in this PWS; and is responsible for performing all the work required to meet the performance metrics and deliver the outputs.

The Contractor is accountable and responsible for the Information Transport, Network Distribution, Computing Services, Application Services, Technical Management, and Information Assurance service categories in the N-NC Service Catalog per the Roles and Responsibility (RACI) matrices for each service. For the COCOM Mission Service category, the Contractor is accountable and responsible for the Service Desk function and Service Operations (Tier 1 responsibilities), in addition to the Technical Management for the supporting services such as Information Transport and Network Distribution that COCOM Mission Services have dependencies.

The Contractor will provide all levels of maintenance and support, as defined in paragraph 2.1 of this PWS. Contracted services include, but are not necessarily limited to, ITIL v3 processes and functions supporting IT Service Strategy Support, Service Design, Service Transition, Service Operations, and Continual Service Improvement. Specific functions include Service Desk, IT Operations, Technical Management, and Applications Management.

This contract includes such tasks as: IT planning, IT projects, IT design, testing and validation, component installation, component diagnostics/troubleshooting, component repair/replacement, enterprise network management, hardware and software handling/accountability, procurement, technical refresh, network administration, systems administration, storage administration, enterprise network and security operations, telecommunications, configuration control and management, enterprise modeling and simulation, visual information/video teleconferencing, information assurance/computer network defense, service desk, user training, world wide web applications, exercise, and support for national special security events.

This contract will support changes to IT Services as identified in the NORAD and USNORTHCOM Service Catalog. Government approved projects will be included in the Service Pipeline to provide new or significantly changed services to the enterprise baseline IT Services. The Government retains the right to identify projects that will be supported by this contract.

During the normal execution of this contract it is expected that the Contractor will identify upgrades and service changes to improve the utility and warranty of IT Services in an effort to reduce total cost of ownership and increase efficiencies. These proposed changes will be handled through the NORAD and USNORTHCOM ITSM Division Change Management process. The Government retains the right to categorize a Request for Change (RFC) as a project. However, changes to services in the N-NC Service Catalog that maintains the utility and warranty of that service is considered in scope of this contract as normal sustainment, and the Contractor is expected to recommend implementation in accordance with industry best practices without imposing additional labor cost upon the Government. This at a minimum includes but not limited to application upgrades covered under software assurance agreements, technical modernization of service assets, and replacing service assets that are nearing end of life.

All process outputs identified in this PWS are the Contractor’s responsibility to maintain through IT Knowledge Management. The Technical Library contains Government output specifications

The Government retains the right to bring in external and/or third party Contractors to perform independent auditing and analysis functions on the existing enterprise, to review any Contractor provided products, and implement new or significant changed service requirements.

Under Commander or Chief of Staff written declaration of urgent and compelling circumstances, capabilities may be identified which require new services to be added to the service catalog or significant increase to existing IT Services as a contract modification under a separate project Contract Line Item Number (CLIN).

1.2.1 Estimated Workload

The work to be performed for all PWS tasks is Firm-Fixed Price. For the specified Optional Tasks the Government requires that the Contractor bid and provide pricing for each Optional Tasks. The Government will retain the right to execute Optional Tasks based on available resources and mission requirements.

1.3 Background and Objective

1.3.1 Background

The NORAD and USNORTHCOM ITSM environment currently consists of support for the Nonsecure Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), SIPRNet Releasable (SIPR-REL), and the classified US and Canadian NORAD Enterprise Network (NEN), CENTRIXS, and commercially provisioned unclassified networks. Support occurs mainly at Peterson AFB in Colorado Springs, CO, but is also required at various locations in the NORAD AOO and NORTHCOM AOR as defined in Par 8.2 Place of Performance.

Depending on the current operational environment, N-NC/J6 provides support to approximate quantities of workstations, blade PCs, printers, servers, infrastructure component, and communications devices (e.g. smart phones, cell phones, and Secure Mobile Environment - Portable Electronic Devices (SME-PED)) across the NIPRNet, SIPRNet, SIPR-REL, and NEN networks.   N-NC/J6 also provides an average of 350-400 Video Teleconferences (VTCs) per month. Refer to the Service Asset Summary for Networks in the Technical Library.

1.3.2 Approximate N-NC IT Environment

The current number of active users ranges between 6,500 and 6,800 depending on status of Battle Staff operations, with approximately 250-300 of those users designated as Priority 1A, 75-100 Priority 1 users, and 50-75 as Priority 2 users. The remaining users are designated as Priority 3 users. Definitions and response requirements for all four categories are outlined in Para 2.3 ITSM Prioritization Levels.

Enterprise information assurance tasks for both network and stand-alone systems vary depending on subordinate and component locations and individual ITSM support cells. However, oversight for monitoring and reporting for the enterprise (e.g. Headquarters (HQ), subordinates, components, ODCs) is the responsibility of NORAD and USNORTHCOM HQs, along with oversight for execution. Service Assets currently on the N-NC Enterprise Network to include applications, systems, and hardware, proprietary and unique Government systems and applications, are in the Hardware and Software Service Asset Catalogs as part of the Technical Library.

Service Desk Requests are currently submitted using email, portal forms, walk-ups, or telephone and are recorded and tracked, as with trouble tickets. Averages of 2,700 service desk requests are submitted per month. For incident an average of 1,200 incident records are submitted by users each month.   On average there are a combined 1,500 combined standard and non standard requests.

NORAD and USNORTHCOM has experienced an average 2-3% growth per year over the past three years in IT service assets and anticipates the same growth line over the life of this contract.

1.3.3 Objective

The objective of this PWS is to obtain professional, administrative, technical, and management support for the N-NC/J6, Command Control Systems Directorate, to support the enterprise IT services provided by the N-NC/J6 in support of NORAD and USNORTHCOM missions.

Provide IT services to NORAD and USNORTHCOM based on the Industry Best Practices ITIL v3 framework that allows for high-quality, measurable performance of IT services. The Contractor shall meet all NORAD and USNORTHCOM IT requirements for the entire life-cycle of each IT service in all possible operating environments ranging from steady-state day-to-day operations, to exercises, tests, deployed operations, and real-world events.

N-NC/J6 operates under an Information Technology Infrastructure Library (ITIL) version 3 framework. The Contractor's quality of work will be assessed based on the ITILv3 framework as referenced in the five Information Technology Infrastructure Library (ITIL) v3 books licensed by the Office of Government Commerce (OGC) publications.

2 Definition and Responsibility Clarification.

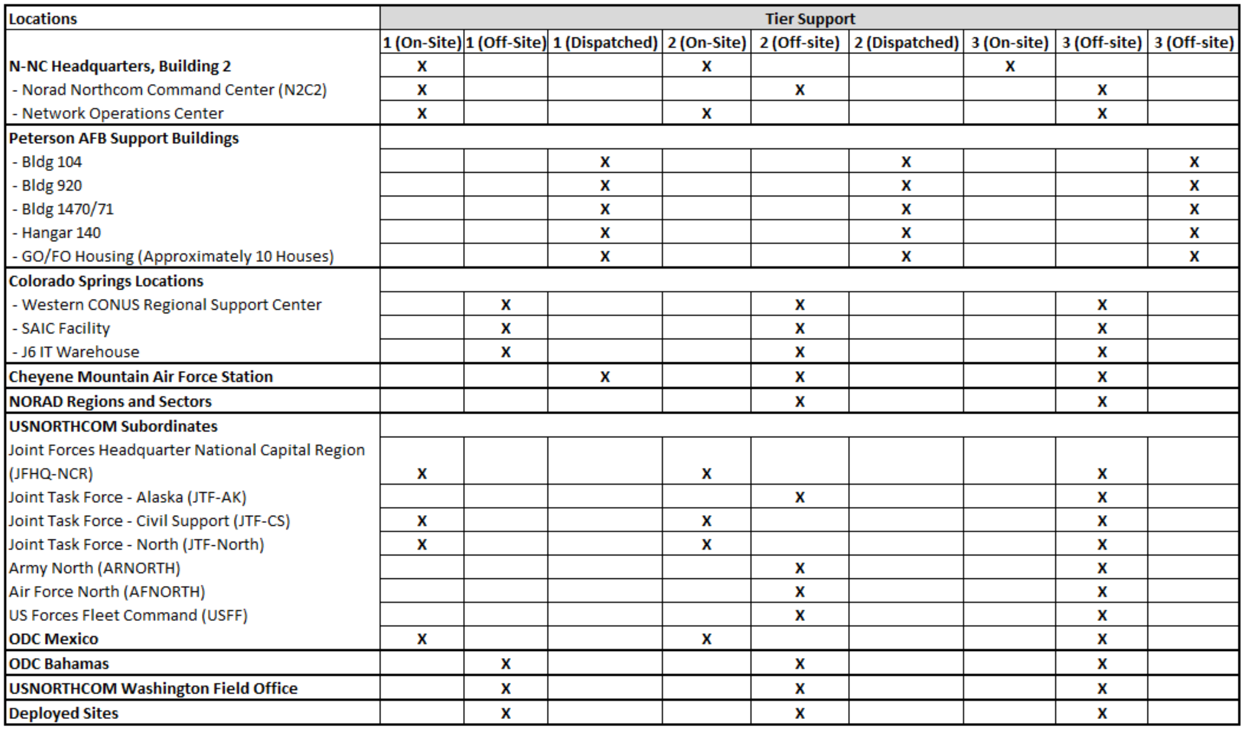
2.1 Enterprise Maintenance Levels

The Contractor is responsible for all levels of maintenance. The Contractor is responsible for the N-NC Enterprise Tier Support as defined in Table 2-1 for on-site, dispatched, and off-site maintenance. These maintenance levels apply to all services in the N-NC Service Catalog and those extended to subordinates, regions, and sectors.

- First-Point Resolution (Tier 1): Performs first look trouble-shooting, including cables, configuration, and customer errors.

- Second-Level Support Group (Tier 2): First point of escalation for problems beyond the scope of the Tier 1 technicians. Would typically include global server configuration settings, security policy, network infrastructure, and application configurations.

- Third-Level Support Group (Tier 3): Final level of escalation for issues beyond the scope of the Tier 2 personnel, including interactions between systems, global network changes, upgrades to newer versions of hardware/software, and third party contracts (e.g. vendors, OEM). Tier 3 support requires that underpinning contracts are in place so Tier 3 personnel can coordinate fixes with the vendor.



Locations	Tier Support								
	1 (On-Site)	1 (Off-Site)	1 (Dispatched)	2 (On-Site)	2 (Off-site)	2 (Dispatched)	3 (On-site)	3 (Off-site)	3 (Off-site)
N-NC Headquarters, Building 2	X			X			X		
- Norad Northcom Command Center (N2C2)	X				X			X	
- Network Operations Center	X			X				X	
Peterson AFB Support Buildings									
- Bldg 104			X			X			X
- Bldg 920			X			X			X
- Bldg 1470/71			X			X			X
- Hangar 140			X			X			X
- GO/FO Housing (Approximately 10 Houses)			X			X			X
Colorado Springs Locations									
- Western CONUS Regional Support Center		X			X			X	
- SAIC Facility		X			X			X	
- J6 IT Warehouse		X			X			X	
Cheyene Mountain Air Force Station			X		X			X	
NORAD Regions and Sectors					X			X	
USNORTHCOM Subordinates									
Joint Forces Headquarter National Capital Region (JFHQ-NCR)	X			X				X	
Joint Task Force - Alaska (JTF-AK)					X			X	
Joint Task Force - Civil Support (JTF-CS)	X			X				X	
Joint Task Force - North (JTF-North)	X			X				X	
Army North (ARNORTH)					X			X	
Air Force North (AFNORTH)					X			X	
US Forces Fleet Command (USFF)					X			X	
ODC Mexico	X			X				X	
ODC Bahamas		X			X			X	
USNORTHCOM Washington Field Office		X			X			X	
Deployed Sites		X			X			X	

Table 2-1. *N-NC Enterprise Tier Support Requirements*

2.1.1 ODC Bahama On-Site Visits

Provide 6 (six) on-site visits per year to ODC Bahamas to provide on-site Tier 1 level maintenance for service asset lifecycle replacement, repair, and survey for ITSM related issues.

2.1.2 (Optional Task) Washington Field Office On-Site Support

(Optional Task) Provide on-site Tier 1 support to the Washington Field Office for approximately 25 users with services identified in the N-NC Service Catalog.

2.1.3 Support Levels

The following support levels apply to locations listed in Table 2-1.

- On-site: Adequate IT support staffing will be housed at these locations as their primary location
- Off-site: Remote support only will be provided to these locations. If on-site support is required, travel costs will be incurred and reimbursable by the government
- Dispatched: While IT support is not housed at these locations, if required, IT support staff will be deployed on-site at no additional cost to the government

2.1.4 N2C2 On-Site Support

Provide on-site Tier 1 – Tier 3 support to approximately 250-300 P1A seats with services identified in the N-NC Service Catalog via a 24x7x365 manned N2C2 Service Desk.

2.2 Maintenance Contracts

2.2.1 Maintenance Contract Procurement

The Contractor will procure maintenance, technical support, warranty, and software assurance as necessary to maintain service levels. The Government, upon approval, will reimburse hardware warranty, software assurance, and telephonic/on-line support, but will not reimburse reinstatement fees, on-site technical support, installation costs, travel expenses, or labor of any kind. If a maintenance contract cannot be severed between maintenance and warranty due to the vendor's pricing model the Contractor will recommend and negotiate the cost to be reimbursed by the Government for the warranty portion. All maintenance contracts required to perform the tasks in this PWS will be bid and executed through a separate Maintenance Contract CLIN.

2.2.2 Government Maintenance Contract Procurement

The Government retains the right to procure maintenance contracts if it is best value or in the best interest of the Government. All existing Government maintenance and warranty contracts are listed in the Technical Library.

2.3 ITSM Prioritization Levels

The following ITSM Prioritization levels are established to support N-NC Enterprise Operations, Users, and Services.

Priority 1A

Priority 1A designation is reserved for Battle Staff Center seats. The seats are associated with the elements identified in the NORAD and USNORTHCOM Publication 1-01 Battle Staff Standard Operating Procedure (BSOP). The primary location for the P1A seats is the NORAD and USNORTHCOM Command Center (N2C2) but the priority designation applies to any location occupied by Battle Staff personnel.

Deployed elements in support of NORAD and USNORTHCOM missions.

Priority 1

Users

General Officer (GO)/Flag Officer (FO)/Senior Executive Service (SES)/Director/Element Commander users.

Services

Mission communications equipment or systems whose failure prevents mission accomplishment.

Mission Critical and Essential services as identified in the N-NC Service Catalog.

All subordinate commands, regions, sectors, and service components that have N-NC services extended to those organizations and if the incident isolates and/or degrades service.

Service outages deemed critical by the appropriate Government Service Owner.

Priority 2

Users

Support staff for GO/FO/SES (Priority 1) users; per the N-NC Chief of Staff's Staff Directory and All command special staff directors.

Services

All subordinate commands, regions, sectors, and service component service provider that have N-NC services extended to those organizations.

Mission communications equipment or systems whose failure prevents mission accomplishment but does not impact Priority 1A and 1 users.

Priority 3

Users

All other N-NC users using N-NC IT Services.

Services

Any request for assistance from a subordinate commands, regions, sectors, and service component service provider that have N-NC services extended to those organizations.

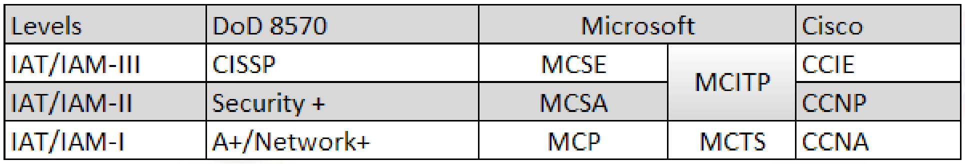
3 Specific Performance Requirements

3.1 Security Clearances and DOD 8570 Compliance

At contract start, the Contractor shall have and maintain sufficient active TOP SECRET (TS)/Sensitive Compartmented Information (SCI) clearances in order to provide support to controlled spaces, to include, but not limited to the Battle Staff Centers per the NORAD and USNORTHCOM Publication 1-01, Battle Staff Standard Operating Procedures (e.g. NORAD and NORTHCOM Command Center (N2C2)) and the N-NC/J6 Network Operations Center, and DR/COOP locations. Ensure access to all supported locations identified for on-site, dispatched, and off-site support per Table 2.1. All other Contractor personnel must have and maintain an active SECRET security clearance.

All Contractor personnel shall:

- Comply with all base and building access cards and escort requirements.
- Report any information or circumstances that may pose a threat to the security of personnel or property.
- Maintain a current listing of all employees and the level of their security clearance.
- Maintain sufficient quantities of contract personnel who are certified in accordance with DOD 8570 and Commercial Certifications as listed in Table 3-1 and other applicable technologies other than Microsoft or Cisco (e.g. EMC Storage Area Network).



Levels	DoD 8570	Microsoft		Cisco
IAT/IAM-III	CISSP	MCSE	MCITP	CCIE
IAT/IAM-II	Security +	MCSA		CCNP
IAT/IAM-I	A+/Network+	MCP	MCTS	CCNA

Table 3-1. DoD 8570 Requirements

- The Contractor shall provide a list to include identification of positions performing IA duties, IA level (e.g. IAT1, IAM1), certification required and certification held for each IAT level per Table 3-1.

3.2 Task Order Description

N-NC/J6 operates under an ITIL v3 framework to plan, develop, design, deliver, maintain, and improve IT Services.

The tasks, requirements, and performance measurements are organized to match the ITIL v3 framework for IT Service Management. The Contractor shall provide, integrate, and manage ITSM Services using industry best practices under the ITIL(v3) framework.

The Contractor is expected to have ITILv3 certified key personnel and staff to perform the services in this PWS.

Requirements for performance measurements and metrics are specified within each process and/or function.

3.3 Task 1: Process Requirements

3.3.1 Sub-Task 1: Process Models

The Contractor Shall:

3.3.1.1 Immediately, at contract start date, execute all processes and producing all required outputs. The Contractor shall produce an Implementation Plan within 30 days after contract award, to demonstrate the Contractor's approach to meet the PWS requirements, to include at a minimum: systems to be used for automation, map all processes/functions to systems the Contractor intends to use to automate the processes and produce the metrics, staffing plan to include at a minimum; DODD 8570 certifications and computing environment certifications, ITIL v3 certifications, and organizational structure to include service and process owners. **[CDRL A001]**

3.3.1.2 Execute ITIL-based process models, based on the ITIL v3 framework, for each of the identified ITIL processes and functions in this Performance Work Statement. The Contractor is accountable and responsible for all aspects of each process and function; the primary interaction between the Contractor and Government is in the form of process outputs. Contractor performance shall be measured using the Operational Metrics (OMs), Key Performance Indicators (KPIs) and Critical Success Factors (CSFs) listed for each process and function.

3.3.1.3 Accountable for the performance of all ITIL processes and functions, that are in scope of this Performance Work Statement, for each Core Service and Service Level Package in the N-NC Service Catalog unless otherwise specified by an accompanying service RACI information matrix (Responsible, Accountable, Consulted, Informed) in the N-NC Service Catalog.

3.3.1.4 Provide Contractor's process model documentation within 30 days after the contract start date. Figure 3-1 depicts the ITIL process model required by NORAD and USNORTHCOM, and represents the framework for each process. The Contractor-provided process models must include, at a minimum, Process Control and Enabler elements, Process Activities, Process Metrics (these are separate and distinct from the PWS metrics), Process Roles to include Responsibility Assignment Matrix – RACI (Responsible, Accountable, Consulted, Informed), Process Procedures, Process Work Instructions, and Process Improvements. Contract process models will be added and maintained in a Contractor IT Knowledge Management System (KMS) and updated as required. **[CDRL: A002].**

3.3.1.5 Ensure processes to conform to approved Government policy and/or IT governance. In lieu of any approved Government policy and/or IT governance the Contractor shall apply expertise and industry best practice to establish policy for each process that governs, at a minimum, Contractor responsibilities. Any Contractor established policy that impacts N-NC customers and/or users will require Government approval (e.g. Change Advisory Board).

3.3.1.6 Responsible for the full service IT lifecycle management (service concept through retirement) for all services in the N-NC Service Catalog. The N-NC Service Catalog identifies which services have Third-Party responsibilities. The Contractor will report to the Government if Third-Party services do not meet their technical management responsibilities.

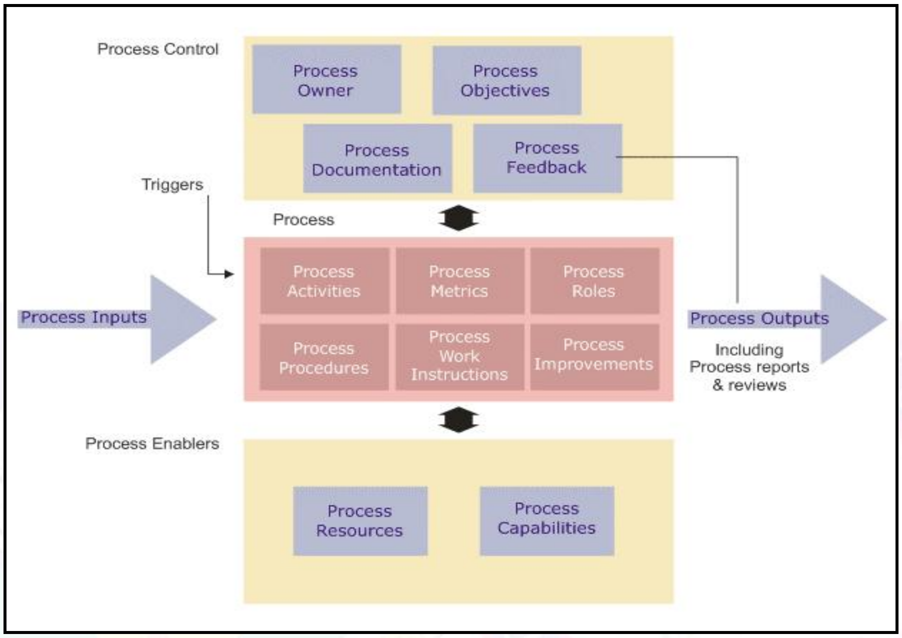


Figure 3-1. NORAD and USNORTHCOM Required Process Model

3.3.2 Sub-Task 2: Process Outputs

3.3.2.1 Operational Metric, Key Performance Indicators, Critical Success Factors

The Contractor Shall:

3.3.2.1.1 Report all Operational Metrics, Key Performance Indicators (KPI), and Critical Success Factors (CSF) for all processes and functions within 30 days after the contract start date and on the 5th business day for each month thereafter. The Contractor will be assessed on the KPIs and CSFs after 30 days of contract start date and on a monthly basis for the life of the contract.

3.3.2.1.2 Automate Operational Metrics (OM) and Key Performance Indicators (KPI) for all processes and functions within 90 days of the contract start date. Key Performance Indicators are calculated based on the OMs, then Critical Success Factors (CSF) are evaluated based on the KPIs associated to them. The CSFs are used to determine the Contractor's performance on this PWS.

3.3.2.1.3 Produce a portal-based dashboard in the N2ITSM environment that automatically pulls raw data from an original record source, calculates the Operational Metrics for a variable time period, and displays Operational Metrics, Key Performance Indicators, and Critical Success Factors without a human intervention. Once the dashboard is connected to the source data and the programming necessary to calculate and display the metrics are complete, the dashboard shall provide near real-time metric results for the current reporting period and the ability to display historical performance without any human intervention or assistance. The Contractor shall document each operational metric specifying the data source, fields and the mathematical model by which the OM is calculated. The dashboard shall have a drill down capability that will enable any dashboard user the ability to automatically display the source data for any metric displayed for any performance time period in order to support Government audit requirements.

3.3.2.2 Output Specifications

The Contractor Shall:

3.3.2.2.1 Ensure outputs conform to the Government output specifications provided in the Technical Library. Quality and completeness of process outputs will be compared to and assessed against the Government output specifications when available. Outputs without a corresponding output specification will be benchmarked against the ITIL v(3) framework.

3.3.2.2.2 Provide outputs that are timely, provided to Government when required; useable, provide meaningful information with all output elements completed; and actionable, the Government can make decisions or take actions based on the output delivered.

3.3.2.2.3 Provide the As Needed outputs immediately after the contract start date when required or when triggered by the output specification default.

3.3.2.2.4 Provide Monthly outputs for each process within 30 days after the contract start date and monthly thereafter. All Monthly outputs will be delivered on the 5th business day of each month.

3.3.2.2.5 Provide outputs with definitive delivery dates on the dates specified in the output specifications.

3.4 Task 2: Service Operations

3.4.1 Sub-Task 1: Service Desk

3.4.1.1 Overview

The Service Desk is a functional unit with personnel involved in differing service events. The Service Desk is the primary point of contact for users experiencing a service disruption or requesting a service request and/or a service change. The Service Desk will provide support to meet the Hours of Work specified in Para 8.1 of this PWS.

The goal of the Service Desk is to provide incident management and request fulfillment. Incident management resumes normal service to the user as soon as possible and documents and facilitates request fulfillment.

3.4.1.2 Requirements

The Contractor Shall:

3.4.1.2.1 Provide, integrate, and manage Service Desk function to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.1.2.2 Maintain the Service Desk as the primary point of contact for all incoming calls (i.e., walk-in, phone call, email, web) for the command to provide a customer focused interface between the users to enable the efficient use of IT services, assisting in the restoral of normal services as soon as possible in addition to being proactive in advising users to potential service interruptions.

3.4.1.2.3 Ensure all service desk requests that are identified as standard requests are immediately processed based on approved request models and nonstandard requests are logged and routed for contractor portfolio analysis.

3.4.1.2.4 Provide accurate status updates and feedback on all service and change requests submitted to the Service Desk on a weekly basis or when contacted by the user, until fulfilled or officially declined.

3.4.1.2.5 Utilize an incident, request and call management database to log, categorize, and escalate incident records as well as record workarounds, maintain a known error database, and document final resolution within required timelines. Expose a customer facing view of the database to allow all N-NC customers (to include subordinates, regions, and sectors) to check on the status of requests in real-time.

3.4.1.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Service Desk Call Report **[CDRL A003]**

3.4.1.4 Operational Metrics

A. Total Number Of Incident Calls Recorded By Service Desk
B. Average Call Duration (Minutes)*
C. Average Waiting Time (Seconds) *
D. Number Of Calls Abandoned after 60 Seconds*
E. Total Number Of First Call Resolution Tickets, within 15 minutes
F. Total Number Of Calls Received
Note * – Provided by base communications support

3.4.1.5 Key Performance Indicators

3.4.1.5.1 Average Call Duration (Minutes) [Metric: B]

- *Superior Service Threshold:* 5 minutes
- *Service Warning:* 10 minutes

3.4.1.5.2 Call Abandon Rate [Metric: D/F]

- *Superior Service Threshold:* 3%
- *Service Warning:* 5%

3.4.1.5.3 Call Waiting Rate [Metric: C]

- *Superior Service Threshold:* (60 seconds)
- *Service Warning:* (120 seconds)

3.4.1.5.4 First Call Resolution Rate [Metric: E/A]

- *Superior Service Threshold:* 70%
- *Service Warning:* 55%

3.4.1.6 Critical Success Factors

- Maintain Quality IT Services [KPI: 1, 2, 3]
- Improve User Satisfaction [KPI: 1, 2, 3, 4]
- Effective Communications with Users [KPI: 1, 4]

3.4.2 Sub-Task 2: Incident Management

3.4.2.1 Overview

Incident management covers every occurrence that disrupts or might disrupt a network, system, capability, or security service. This includes incidents reported by customers to the Service Desk as well as those reported by the technical staff, sites, and automated systems.

The goal of Incident Management is to restore normal service operation as quickly as possible and minimize the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

3.4.2.2 Requirements

The Contractor Shall:

3.4.2.2.1 Provide, integrate, and manage Incident Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.2.2.2 Apply the following ITSM Prioritization Levels to incident management. By exception, the Director/Deputy Director of Command and Control Systems, can elevate the priority of an operations element, staff section, and/or individual for a temporary period of time to meet an urgent or critical command need and if there is a significant impact to meet the mission.

Priority 1A

Priority 1A designation is reserved for Battle Staff Center seats. The seats are associated with the elements identified in the NORAD and USNORTHCOM Publication 1-01 Battle Staff Standard Operating Procedure (BSOP). The primary location for the P1A seats is the NORAD and USNORTHCOM Command Center (N2C2) but the priority designation applies to any location occupied by Battle Staff personnel.

Deployed elements in support of for NORAD and USNORTHCOM missions (e.g. Homeland Defense, Civil Support, and National Special Security Event (NSSE)).

- Restoral of service within 2 hours with a 30 minute response

Priority 1

Users

Bldg 2: General Officer (GO)/Flag Officer (FO)/Senior Executive Service (SES)/Director/Element Commander users

The contractor shall restore service within 4 hours. Service restoration shall be contingent upon a required time coordinated with the executive staff. Based on an 0600-1800 business day.

Services

Mission communications equipment or systems whose failure prevents mission accomplishment

Mission Critical and Essential services as identified in the N-NC Service Catalog

All subordinate commands, regions, sectors, and service components that have N-NC services extended to those organizations and if the incident isolates and/or degrades service.

Service outages deemed critical by the appropriate Government Service Owner

All require restoral of like service capability within 4 hours

<u>Priority 2</u>

Users

Support staff for GO/FO/SES (Priority 1) users; per the N-NC Chief of Staff's Staff Directory and All command special staff directors.

- Restoral of service within 12 hours based on 0600-1800 business day

Services

All subordinate commands, regions, sectors, and service component service provider that have N-NC services extended to those organizations.

Mission communications equipment or systems whose failure prevents mission accomplishment but does not impact Priority 1A and 1 users.

All require restoral of like service capability within 12 business hours

<u>Priority 3</u>

All other N-NC users using N-NC IT Services.

Any request for assistance from a subordinate commands, regions, sectors, and service component service provider that have N-NC services extended to those organizations

3.4.2.2.3 Manage, configure, install, troubleshoot, maintain and upgrade Government-approved incident management systems. Make the incident management system available for Government access, use, and review at all times.

3.4.2.2.4 Respond and resolve all incidents for N-NC users. On average Priority 1A user incidents will be responded to in 30 minutes and resolved in 2 hours; Priority 1 user incidents will be resolved within 4 hours; Priority 2 user incidents will be resolved within 12 business hours. Priority 3 user incidents will be resolved within 36 business hours. To minimize the incident aging, ninety percent (90%) of Priority 3 user problems will be resolved within 3 (three) business days, and one-hundred percent (100%) of Priority 3 user problems will be resolved within 10 business (i.e. these requires all Priority 3 tickets to be resolved in 10 business days). All user incidents not resolved within 10 business days will be reported daily in the Daily Service Desk Report.

3.4.2.2.4.1 Contact end-user on any anticipated service level breaches based on end-user priority. The customer must agree that the incident is resolved prior to closure.

3.4.2.2.4.2 All open incidents, at the time of the contract start date, will be reported within 10 business days of contract start. Incident open dates will be reset to contract start date and resolved IAW the ITSM prioritization schema.

3.4.2.2.5 Report all major incidents defined by either a service outage or degradation affecting 10 or more users or a Core Service outage within 30 minutes to the Government Service Owner and/or management. Produce a major incident model for each Core Service Package.

3.4.2.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Incident Management Report **[CDRL A003]**
2. SLA/OLA Breach Report
3. Major Incident Report

3.4.2.4 Operational Metrics

A. Total Number Of Incidents (All incidents resolved)

B. Number Of Incidents Resolved Within Priority Levels
C. Number Of Incidents Reopened Within 10 Working Days
D. Incidents Caused By Customer (e.g., Port Blocked Denial of Service, Password Lock Out)
E. Number Of Closed Incidents without Customer/User Agreement
F. Total Number of Incidents Using Generic Incident Model
G. Number of Priority 3 Incidents Resolved within 36 Business Hours
H. Number of Priority 3 Incidents Resolved
I. Average Time to Incident Resolution for Priority 1A User
J. Average Time to Incident Resolution for Priority 1 User
K. Average Time to Incident Resolution for Priority 2 User
L. Average Time to Incident Resolution for Priority 3 User

3.4.2.5 Key Performance Indicators

3.4.2.5.1 Incident Resolution Rate [Metric: (B/A)]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.4.2.5.2 Customer Incident Impact Rate [Metric: (D/A)]

- *Superior Service Threshold:* 4.5%
- *Service Warning:* 7.5%

3.4.2.5.3 Incident Reopen Rate [Metric: (C/A)]

- *Superior Service Threshold:* 4.5%
- *Service Warning:* 7.5%

3.4.2.5.4 Customer Dissatisfaction Rate [Metric: (E/A)]

- *Superior Service Threshold: 5%*
- *Service Warning: 10%*

3.4.2.5.5 Incident Resolution (Avg) for Priority 1A Users [Metric: I]

- *Superior Service Threshold:* 1 hour (Average)
- *Service Warning:* 2 hours (Average)

3.4.2.5.6 Incident Resolution (Avg) for Priority 1 Users [Metric: J]

- *Superior Service Threshold:* 2 business hours (Average)
- *Service Warning:* 4 business hours (Average)

3.4.2.5.7 Incident Resolution (Avg) for Priority 2 Users [Metric: K]

- *Superior Service Threshold:* 8 business hours (Average)
- *Service Warning:* 12 business hours (Average)

3.4.2.5.8 Incident Resolution (Avg) for Priority 3 Users [Metric: L]

- *Superior Service Threshold:* 36 hours (Average)
- *Service Warning:* 72 hours (Average)

3.4.2.5.9 Incident Model Utilization Rate [Metric: F/A]

- *Superior Service Threshold: 95.0%*
- *Service Warning: 85.0%*

3.4.2.5.10 Priority 3 Incident Aging [Metric: G/L]

- *Superior Service Threshold: 90%*
- *Service Warning: 80%*

3.4.2.6 Critical Success Factors

- Provide Effective and Efficient IT Service Management [KPI: 1, 3, 4, 9, 10]
- Maintain Quality IT Services [KPI: 1, 2, 3, 4]
- Improve Mission/Business Productivity with IT Services [KPI: 1, 2, 3, , 9]
- Improve User Satisfaction [KPI: 1, 2, 3, 5, 6, 7, 8, 9]

3.4.3 Sub-Task 3: Request Fulfillment

3.4.3.1 Overview

Request Fulfillment is the process that incorporates all aspects of fulfilling a customer's Government approved request. User requests can be requests for information, advice, a standard change, or access to a service in the IT Service Catalog. It should include self-service for identifying available services, capture the service request, approval, tracking, provisioning, delivery and delivery confirmation.

The goals of the Request Fulfillment process are:

- To offer users a channel through which they can request and receive services; to this effect an agreed approval and qualification process must exist
- To provide users and customers with information about the availability of service and the procedures for obtaining these services
- To assist with general information, complaints, or comments

3.4.3.2Requirements

The Contractor Shall:

3.4.3.2.1 Provide, integrate, and manage Request Fulfillment to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical

Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.3.2.2 Apply the following ITSM Priority Levels to request fulfillment. By exception, the Director of Command and Control Systems, can elevate the priority of an operations element, staff section, and/or individual for a temporary period of time to meet an urgent or critical command need and if there is a significant impact to meet the mission.

3.4.3.2.3 Manage, configure, install, troubleshoot, maintain and upgrade Government-approved service request management systems. Make the service request management system available for Government access, use, and review at all times.

3.4.3.2.4 Respond and resolve all service requests for N-NC users and customers. Estimated average 1,500 service requests per month, both standard and non standard.

3.4.3.2.4.1 On average Priority 1A requests will be fulfilled in 3 (three) business days; Priority 1 user requests will be fulfilled within 5 business days; Priority 2 user requests will be fulfilled within 10 business days. Priority 3 user requests will be fulfilled within 14 business days. All Priority 1A, 1, and 2 service requests exceeding the specified fulfillment days will be reported daily. These fulfillment requirements may be superseded by a Government approved request models that specify fulfillment days other than those identified.

3.4.3.2.4.2 All open service requests, at the time of the contract start date, will be reported within 10 business days of contract start.

3.4.3.2.5 After 30 calendar days of contract start the Contractor shall produce a standard request model for the top requests according to volume, recommended changes and update to these request models shall be made quarterly.

3.4.3.2.6 Produce a Request Model for each IT Service. A Request Model should include, at a minimum, approval authority, provisioning steps, associated costs, funding approval steps, service assets, the Core Service Package and any associated Service Level Package(s) for any differentiated offerings. Each Request Model will be approved by the Change Advisory Board prior to it becoming a standard change.

3.4.3.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Request Fulfillment Report **[CDRL A003]**

2. Request Model for each IT Service

3.4.3.4 Operational Metrics

A. Average Time to Fulfill Requests for Priority 1A User
B. Average Time to Fulfill Requests for Priority 1 User
C. Average Time to Fulfill Requests for Priority 2 User
D. Average Time to Fulfill Requests for Priority 3 User
E. Number Of Request Fulfillment Complaints
F. Total Number of Requests
G. Number of Service Requests Using Generic Request Models
H. Number Of Requests Reopened

3.4.3.5 Key Performance Indicators

3.4.3.5.1 Request Fulfillment Rate for Priority 1A Users [Metric: A]

- *Superior Service Threshold:* 2 business days (Average)
- *Service Warning:* 3 business days (Average)

3.4.3.5.2 Request Fulfillment Rate for Priority 1 Users [Metric: B]

- *Superior Service Threshold:* 3 business days (Average)
- *Service Warning: 5 business days (Average)*

3.4.3.5.3 Request Fulfillment Rate for Priority 2 Users [Metric: C]

- *Superior Service Threshold: 7 business days (Average)*
- *Service Warning:* 10 business days (Average)

3.4.3.5.4 Request Fulfillment Rate for Priority 3 Users [Metric: D]

- *Superior Service Threshold:* 10 business days (Average)
- *Service Warning:* 14 business days (Average)

3.4.3.5.5 Request Fulfillment Satisfaction Rate [Metric: 1-(E/F)]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.4.3.5.6 Service Request Reopen Rate [Metric: H/F]

- *Superior Service Threshold: 3.0%*
- *Service Warning: 5.0%*

3.4.3.5.7 Request Model Utilization Rate [Metric: G/F]

- *Superior Service Threshold: 95.0%*
- *Service Warning: 85.0%*

3.4.3.6 Critical Success Factors

- Deliver Accurate and Timely IT Services [KPI: 1, 2, 3, 4, 5, 7]
- Maintain Quality IT Service [KPI: 1, 2, 3, 4, 5,7]
- Improve User Satisfaction [KPI: 1, 2, 3, 4, 5, 6, 7]

3.4.4 Sub-Task 4: Access Management

3.4.4.1 Overview

Access Management consists of the processes and procedures responsible for allowing users to make use of IT services, systems, applications, data, or other IT assets. Access Management helps to protect the Confidentiality, Integrity and Availability of assets by ensuring that only authorized users are able to access or modify the assets.

The goal of Access Management is to ensure internal and external users have the appropriate level of access to a service, but differs from Availability Management in that it does not guarantee that access is always available at the agreed times.

3.4.4.2 Requirements

The Contractor Shall:

3.4.4.2.1 Provide, integrate, and manage Access Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.4.2.2 Ensure that access rights are terminated or restricted upon death, resignation, dismissal, role change, and transfer or travel where different regional access applies (system, network and physical).

3.4.4.2.3 Change administrator passwords and service accounts on all NORAD and USNORTHCOM Enterprise computer and network communications systems in accordance with DoD and NORAD and USNORTHCOM password policies. Document service account passwords and detailed procedures involved in changing the passwords for each service in a physical password book. Maintain a physical copy at both Peterson AFB and CMAFS.

3.4.4.2.4 Coordinate with Telephone Control Officers on a monthly basis to ensure users of smart phones, cell phones, and other wireless devices are still active and assigned to the command to ensure wireless accounts are not continued after a user is terminated, transferred, and/or released from the command.

3.4.4.2.5 Maintain documentation of all users with elevated rights including system, network and storage administrators, specific rights delegated to and/or roles held by each user and service account.

3.4.4.2.6 Maintain and manage elevated privileges. Users with elevated privileges will have a valid requirement for such and meet all required certification and training prior to being granted any elevated privileges. The Government retains the right to review, approve, disapprove, and audit Contractor personnel with elevated access and privileges.

3.4.4.2.7 Conform to Department of Defense Directive (DoDD) 8570.01-M, Information Assurance Workforce Improvement Program 8570 IT security and system specific certification requirements for granting elevated access privileges. Ensure that all personnel with elevated access are commercially certified on each service asset they have elevated access to relative to their labor category. For service assets without a formal certification program course completion of relevant training is sufficient. Personnel must also obtain the required DoDD 8570 Security certification corresponding to the labor category. Maintain a personnel database with all required certification information and make the database available to the Government.

3.4.4.2.8 A master list of passwords shall be maintained in a secure location. Access to the secure location shall be provided to the Government.

3.4.4.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Access Management Report **[CDRL A003]**
2. Unauthorized Access and Rights Escalation Report
3. Quarterly Access Management Report **[CDRL A006]**

3.4.4.4 Operational Metrics

A. Total Number Of Services
B. Number Of Services With Corresponding Access Policy
C. Total Number Of Service Desk Initiated Access Related Incidents
D. Total Number Of Incidents
E. Total Number Of User (Non-Service) Accounts Over 30 Days Inactive
F. Total Number Of User (Non-Service) Accounts Over 30 Days Inactive Not Disabled
G. Total Number of User (Non-Service) Accounts Over 90 Days Inactive
H. Total Number of User (Non-Service) Accounts Over 90 Days That Do Not Have a Waiver

I. Total Number Of Service Accounts
J. Total Number Of Service Accounts Passwords Greater Than 365 Days Without Government Approval
K. Total Number of N2ITSM Contractors filling positions requiring DODD 8570 Certification
L. Number of N2ITSM Contractor staff with required DODD 8570 Certification
M. Total Number of staff (Non-N2ITSM Contractor staff) with elevated rights, filling positions requiring DODD 8570 Certification
N. Number of staff (Non-N2ITSM Contractor staff) with elevated rights, with required DODD 8570 Certification

3.4.4.5 Key Performance Indicators

3.4.4.5.1 Access Policy Coverage Ratio [Metric: B/A]

- *Superior Service Threshold:* 98.0%
- *Service Warning:* 90.0%

3.4.4.5.2 User Impact Rate [Metric: C/D]

- *Superior Service Threshold:* 2.0 %
- *Service Warning:* 10.0%

3.4.4.5.3 Access Revocation Rate [Metric: F/E]

- *Superior Service Threshold:* 2.0%
- *Service Warning:* 10.0%

3.4.4.5.4 Account Deletion Rate [Metric: H/G]

- *Superior Service Threshold:* 2.0%
- *Service Warning:* 10.0%

3.4.4.5.5 Service Account Access Management [Metric: J/I]

- *Superior Service Threshold:* 2.0%
- *Service Warning:* 10.0%

3.4.4.5.6 N2ITSM Contractor DODD 8570 Compliance [Metric: L/K]

- *Superior Service Threshold: >95.0%*
- *Service Warning: <75.0%*

3.4.4.5.7 Non-N2ITSM Contractor DODD 8570 Compliance [Metric: N/M]

- *Superior Service Threshold: >95.0%*
- *Service Warning: <75.0%*

3.4.4.6 Critical Success Factors

- Improve User Satisfaction [KPI: 3, 4]
- Maintain IT Security Compliance [KPI: 1, 2, 5, 6, 7]
- Protect and Defend IT Service from Threats [KPI: 1, 4, 5]

3.4.5 Sub-Task 5: Technical Management – Network and Infrastructure

3.4.5.1 Overview

Technical Management manages day-to-day technical support functions within NORAD and USNORTHCOM and refers to the group that provides technical expertise and overall management of the NORAD and USNORTHCOM IT Enterprise. Technical management also plays an important role in the design, testing, training, release and improvement of IT Enterprise services.

The goal of Technical Management is to apply technical expertise to meet or exceed agreed service levels for all NORAD and USNORTHCOM Enterprise services.

3.4.5.2 Requirements

The Contractor Shall:

3.4.5.2.1 Provide, integrate, and manage Technical Management function to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors. The Government will review and validate reports and documents provided by the Contractor and provide feedback. Report to government Service Owner and senior management on all infrastructure and service issues relevant to their area of responsibility.

3.4.5.2.2 Be Accountable for Technical Management of the services in the N-NC Service Catalog, Appendix D of this PWS, except for those COCOM Mission Services with an accompanying RACI matrix. The Contractor is accountable, responsible, or consulted for specific processes, functions, and service dependencies identified by N2ITSM Contractor in the RACI for each service in the N-NC Service Catalog.

3.4.5.2.3 Provide remote Tier 3 support for all N-NC Services extended to those subordinates, components, regions, and sectors organizations identified in the N-NC Service Catalog. Those organizations are identified as ‘’locations” in the N-NC Service Catalog. The Contractor is expected to provide support, per Table 2-1 of this PWS, to those locations as required to maintain service levels.

3.4.5.2.4 Provide network, server, Storage Area Network (SAN), database administration for the NORAD and USNORTHCOM enterprise which includes the SIPRNET, SIPR-REL, NIPRNET, NEN, CENTRIX, and Technology Integration Lab networks.

3.4.5.2.5 Perform COMSEC Responsible Officer duties and adhere to and support all COMSEC policy as they relate to support and maintenance of N-NC Networks and C4 Operations. Document COMSEC assets in the Communications Security Custodians Report. Provide cryptographic support and shall install, operate, and key all cryptographic items attached to the N-NC networks; Primarily but not limited to STE, KOV 14s, KIV 7, KG-75, KG-175, KG-250, TALON, SECNET-54 and other NSA approved Type I cryptographic devices.

3.4.5.2.6 Perform Circuit Management Office duties. Procure and manage long haul telecommunications services and circuits between the command, DISA, AFCA and others. Writes, assists subordinates in writing, reviews and validates all Telecommunications Requests (TR). Executes, or assists in executing, the programming and budgeting of long haul telecommunications for the command and its subordinates. Tracks all long haul telecommunications expenditures for services provisioned through DISA and the Defense Information Technology Contracting Office. Tracks all circuit actions for the N-NC Enterprise. Maintains Circuit History Folders and a circuit database for all circuits and services provisioned through DISA. There are approximately 150 active circuits. Track monthly expenditures for GIG circuits and services. Provide the circuit expenditures as part of the Monthly ITSM Budget Report . Create and maintain Circuit History Folders in accordance with AFI 33-116, Para 3.3. Create within sixty days of the start of the contract and maintain the Circuit Database for N-NC Enterprise. Create and maintain a method for tracking all circuit actions within the N-NC Enterprise. Ensure that all active and requested circuits information is made available to the Network Service Owners as needed.

3.4.5.2.7 Video Tele-Conference (VTC), Audio/Visual (AV), and Community Access TV (CATV). Install, operate, and maintain the VTC, AV, and CATV capabilities in the N-NC HQs and CMAFS to include the VTC capabilities, video wall systems, video matrix switches, CATV, Public Announcement systems, Command Displays, Conference Room Audio/Video, and other audio/video capabilities. Provide after action reports on all VTCs upon request of the Government. Provide integration and convergence of voice, data, and video solutions for current and future VTC protocols. Establish monitoring and reporting on all critical network components and provide trend analysis reports and provide reports upon Government request. Provide additional functional and technical support to respond to short notice requirements and work non-standard hours to include 24/7 operations. For Top-4 VTCs (N-NC CDR, NC Deputy CDR, NORAD Deputy CDR, and Chief of Staff), a VTC Technician is required to be on-site in the conference room for the duration of the VTC to provide technical assistance if required. Provide 45 minute response time for off-duty VTC support (Estimate 3 to 5 times a month).

3.4.5.2.7.1 Operate, maintain, troubleshoot, and upgrade VTC Multipoint Control Unit (MCU) and all associated video equipment to include video distribution systems for Allied, US classified and unclassified conference rooms. Operate a minimum of four simultaneous MCU VTCs, 3 on SIPRNET and 1 on NIPRNET on a 24/7 basis.

3.4.5.2.7.2 (Optional Task) VTC and Conference Room Scheduling. Manage the scheduling of conference rooms requiring VTC and/or IT support. Schedule conference room facilities based on user VTC and/or IT Support requirements and resolve scheduling conflicts. Ensure VTC and/or IT support equipment is functional and operational prior to scheduled use. Monitor VTCs during scheduled meetings to resolve connectivity or VTC functionality issues. Estimate 2,200 VTCs per year.

3.4.5.2.8 Cabling and Wiring. Maintain, install, configure, upgrade, troubleshoot and repair all N-NC Network cabling infrastructure (SIPRNET, SIPR-REL, NIPRNET, NEN, CENTRIX, JWICS, commercial, video) and cable television. Perform Emission Security inspections prior to installation of classified connections and comply with all RED/BLACK switch separation. Test all data Network fiber cabling and ensure they meet industry accepted standards for allowable fiber and Category-6 conductivity. Estimate up to 200 network drop installs, 50 cable TV installs, 200 network drop moves/relocations annually.

3.4.5.2.9 Virtual Infrastructure. Operate, maintain, optimize, and expand the N-NC virtual infrastructure to include virtual servers and virtual desktops, currently using VMware technology. Virtualize servers and workstations to maximum extent possible to reduce maintenance requirement, energy requirements, and/or improve security compliance.

3.4.5.2.10 Data Storage, Continuity, and Back-Up. Ensure the integrity of centrally managed servers and data. Manage, store, dispose of, restore and test backups, clean/maintain backup devices. Maintain, update, and operate enterprise systems to ensure Continuity of Operations (COOP), Disaster Recovery (DR) and contingency support. Manage, configure, troubleshoot, and upgrade the remote N-NC DR replication and fail-over capabilities to include SAN, Exchange Servers, File Servers, Portal Servers, Application Servers, Disk to Disk backup system, archive systems, and DMS/AMHS at the remote DR location. Manage, maintain and restore data archive storage. The Contractor shall review COOP/DR plans cited in associated COOP/DR Annexes provided within the Technical Library and update as changes occur. Create maintain and restore back-ups for system configurations, application, logs and user data.

3.4.5.2.11 Apply all applicable network all Communication Task Orders (CTOs) within the time frame designated by applicable DoDI, CJCSI, and NORAD and USNORTHCOM orders. If the Contractor cannot apply the Orders within the stated suspense, the Contractor shall submit an extension request through the N-NC Theater NetOps Control Center (TNCC).

3.4.5.2.12 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Incident Management required in 3.4.2

3.4.5.2.13 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Problem Management required in 3.4.6

3.4.5.2.14 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Change Management required in 3.8.3

3.4.5.2.15 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Information Security Management required in 3.7.6

3.4.5.2.16 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Availability Management required in 3.7.7

3.4.5.2.17 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Capacity Management required in 3.7.8

3.4.5.2.18 Perform Technical Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for IT Service Continuity Management required in 3.7.9

3.4.6 Sub-Task 6: Problem Management

3.4.6.1 Overview

Problem management comprises all activities needed to diagnose the underlying root cause of incidents and to find a solution for these problems. It also ensures that the solution is implemented using the correct change management and release management processes.

The goal of Problem Management is to minimize the adverse business impact of incidents that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

3.4.6.2 Requirements

The Contractor Shall:

3.4.6.2.1 Provide, integrate, and manage Problem Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.6.2.2 Open a problem record based on, but not limited to incident trending analysis, reoccurring major incidents, and/or event notification indicating a degradation of Service. Problem records can also be opened when directed by the Government.

3.4.6.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Problem Management Report **[CDRL A003]**
2. Monthly Known Error Database (KEDB**) [CDRL A004]**
3. Root Cause Analysis Report(s)

3.4.6.4 Operational Metrics

A. Number Of Repeat Incidents By User/System
B. Total Number Of Incidents
C. Total Number Of Open Problems Records
D. Number Of Problem Records with Workaround and/or Documented Resolution)
E. Number Of Problems Reopened

F. Number Of Repeat Incidents By Category

3.4.6.5 Key Performance Indicators

3.4.6.5.1 User/System Incident Repeat Rate [Metric: A/B]

- *Superior Service Threshold:* 5.0%
- *Service Warning:* 7.0%

3.4.6.5.2 Category Incident Repeat Rate [Metric: F/B]

- *Superior Service Threshold:* 5.0%
- *Service Warning:* 7.0%

3.4.6.5.3 Problem Resolution Rate [Metric: D/C]

- *Superior Service Threshold:* 80%
- *Service Warning:* 65%

3.4.6.5.4 Problem Reopen Rate [Metric: E/C]

- *Superior Service Threshold:* 7%
- *Service Warning:* 12%

3.4.6.6 Critical Success Factors

- Minimize User/Customer Impact to IT Service Disruptions (Reduce Incident Frequency/Duration) [KPI: 1, 2]
- Maintain Quality of IT Services [KPI: 1, 2]
- Provide Effective and Efficient IT Service Management [KPI: 3, 4]

3.4.7 Sub-Task 7: Applications Management – Commercial and Govt Off-the-Shelf

3.4.7.1 Overview

Application Management manages day-to-day system administration functions of applications within NORAD and USNORTHCOM and refers to the group that provides technical expertise and overall management of the applications/systems on the NORAD and USNORTHCOM IT Enterprise. Application management also plays an important role in the design, testing, training, release and improvement of IT Enterprise services. The Application Management function operates and maintains the N-NC software (primarily Commercial Off-the-Shelf (COTS)/Government Off-the-Shelf (GOTS)) as well as daily system administration activities. .

The goal of Application Management is to apply technical expertise to meet or exceed agreed service levels for all NORAD and USNORTHCOM Enterprise services.

3.4.7.2 Requirements

The Contractor Shall:

3.4.7.2.1 Provide, integrate, and manage Applications Management function to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.7.2.2 Be Accountable for Application Management of the services in the N-NC Service Catalog, Appendix D of this PWS, except for those C2 Mission Services with an accompanying RACI matrix. The Contractor is accountable, responsible, or consulted for specific processes, functions, and service dependencies identified by N2ITSM Contractor in the RACI for each service in the N-NC Service Catalog.

3.4.7.2.3 Request for New Software assets or Major version changes (e.g. Adobe v9 to v10) to software not covered under Software Assurance shall be sent to the Government Business Relationship Manager (BRM) to identify Service Level Requirements of Utility and Warranty and funding source.

3.4.7.2.4 Monitor for major application/software version updates (e.g. Adobe v9 to v10) covered under Software Assurance (e.g. contracts or Enterprise License Agreements) and submit a change request for Government approval for the upgrade within 30 days after commercial release. Major version upgrades that increase utility and warranty will be provided to the Government in either a Service Package or Service Improvement Package.

3.4.7.2.5 Monitor for application/software updates which would impact warranty of service assets. Contractor shall submit a change request within 30 days of commercial release or when requested sooner by the Government. These software updates may include minor changes (e.g. v9.1 to v9.2), downward directed JTF-GNO (e.g. CAMS, CTO, Patches, etc.), vendor patches, hot fixes, plug-ins, DLLs, Service Package and service releases.

3.4.7.2.6 Ensure necessary system administration training, awareness and experience levels are maintained within the team or department and provide the same level of training and awareness to government service owners.

3.4.7.2.7 Report to Government Service Owner and Management on all application issues relevant to their area of responsibility.

3.4.7.2.8 Provide application lifecycle management for services and related Service Assets. To include plans to maintain the most current version and patch level of all software applications listed in the N-NC software asset catalog that support core services and service level packages and/or end-user computing services.

3.4.7.2.9 Support and participate in the design, build, and integration of new and/or significantly modified IT services.

3.4.7.2.10 Support application testing plans and deployment plans for all applications releases.

3.4.7.2.11 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Incident Management required in 3.4.2

3.4.7.2.12 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Problem Management required in 3.4.6

3.4.7.2.13 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Change Management required in 3.8.3

3.4.7.2.14 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Information Security Management required in 3.7.6

3.4.7.2.15 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Availability Management required in 3.7.7

3.4.7.2.16 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for Capacity Management required in 3.7.8

3.4.7.2.17 Perform Applications Management tasks to meet Outputs, Operational Metric, KPIs and CSFs for IT Service Continuity Management required in 3.7.9

3.4.8 Sub-Task 8: IT Operations Management

3.4.8.1 Overview

IT Operations is responsible for performing NORAD and USNORTHCOM's day-to-day operational and situational awareness activities for delivering IT services identified in the Service Catalog. It monitors to ensure and report on a secure and stable IT environment that can evolve or adapt to meet the future needs of the NORAD and USNORTHCOM mission and ensures the IT enterprise is reliable, robust, secure, consistent, and facilitates the efficient and effective delivery of services required of this PWS.

The goal of Operations Management is to monitor, manage, assess, and report on NORAD and USNORTHCOM's end-to-end IT enterprise that facilitates the delivery of the IT services to achieve the NORAD and USNORTHCOM missions.

3.4.8.2 Requirements

The Contractor Shall:

3.4.8.2.1 Provide, integrate, and manage IT Operations Management function to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.8.2.2 Comply with all NORAD and USNORTHCOM Cyber Task Orders, Cyber WARNORDs and FRAGOs issued by the N-NC Theater NetOps Control Center (TNCC).

3.4.8.2.3 Create and brief an Executive Summary (EXSUM) and closure report for each major incident. Provide brief to ITSM Division leadership, and relevant Government Process and Service Owner(s).

3.4.8.2.4 Produce a major incident closure report within 24 hours of resolving the incident with key elements briefed to the relevant Government Process and Service Owner(s). Frequently report, or as requested by Government, major incident status and progress.

3.4.8.3Operational Metrics

A. Total Number of Major Incidents
B. Number of Major Incident Closure Reports

C. Number of EXSUM created for Major Incidents
D. Number of Major Incidents Not Triggered by a Monitoring and Reporting tool
E. Total Number of Services in the Service Catalog
F. Number of Services with End-to-End Service Monitoring

3.4.8.4 Key Performance Indicators

3.4.8.4.1 Closure Report Rate [Metric: (B/A)]

- *Superior Service Threshold:* 100%
- *Service Warning:* 90%

3.4.8.4.2 Major Incident EXSUM Rate [Metric: (C/A)]

- *Superior Service Threshold:* 100%
- *Service Warning:* 90%

3.4.8.4.3 Monitoring Major Incident Effectiveness [Metric: (D/A)]

- *Superior Service Threshold:* 10%
- *Service Warning:* 20%

3.4.8.4.4 Service Monitoring Coverage [Metric: (F/E)]

- *Superior Service Threshold: 100%*
- *Service Warning: 80%*

3.4.8.5 Critical Success Factors

- Optimize overall Mission Risks [KPI: 2, 3, 4]
- Demonstrate and Promote IT Service Efficiency [KPI: 1, 2,4]
- Minimize User/Customer Impact to IT Service Disruptions [KPI: 3, 4]

3.4.9 **(Optional Task) Network Operations Center Support**

3.4.9.1 Overview

Perform an IA/Computer Network Defense, network monitoring, compliance, and liaison capability. Provide a watch capability in the Network Operations Center (NOC).

3.4.9.2 Requirements

The Contractor Shall:

3.4.9.2.1 Monitor the health of all N-NC services and report on (e.g. SITREPs, COMSTATs, COMSPOTs) the status of for all security domains (i.e. NIPR, SIPR, NEN, CENTRIXS).

3.4.9.2.1.1 Provide technical and mission impact assessments and liaise with the NOC, TNCC, and CFC for all service outages, incidents, problems, maintenance. Provide status updates and reports until service restoration.

3.4.9.2.1.2 Ensure all network and service monitoring tools specified in the N-NC Service Catalog and Software Catalog are configured, optimized, and tuned to enable proactive network monitoring.

3.4.9.2.1.3 Report to the NOC within 30 minutes the isolation and/or degradation of any N-NC services or networks in the N-NC Service Catalog.

3.4.9.2.2 Comply with USNORTHCOM Communications Task Order (CTO), currently 10-01, for all IA/CND directives to include TASKORDs, CTASKORDs, FRAGOs, WARNOs, IAVAs, and MTOs.

3.4.9.2.2.1 Monitor, track, and report task assignment until completion.

3.4.9.2.2.2 Monitor NIPR and SIPR email for Task-Orders 24/7/365.

3.4.9.2.2.3 Report to the NOC within 60 minutes the loss or degradation of any CND Device at N-NC HQ.

3.4.9.2.2.4 Report to the NOC within 60 minutes the detection of a CND event.

3.4.9.2.3 Monitor, analyze, initiate response, and report on IA/CND events using configured tools. Ensure all IA/CND tools specified in the N-NC Service Catalog and Software Catalog are configured, optimized, and tuned to enable proactive network defense.

3.4.9.2.3.1 Perform traffic analysis and validation, network and system log analysis (.e.g. firewalls, routers, IDS, proxies, directory services, filters)

3.4.9.2.3.2 Respond to IA/CND events by, but not limited to, blocking accounts, network isolation, access control list modification, firewall and IDS changes, etc.

3.4.9.2.4 Participate in operational briefings and meetings to provide situational awareness and status for IA/Computer Network Defense, network monitoring, compliance, and liaison capability.

3.4.9.2.4.1 Participate in J6 Daily Ops Briefing.

3.4.9.2.4.2 Participate in classified NOC Weekly Defense Connect Online (DCO) conferences.

3.4.9.3 Outputs

1. Daily Operations Brief Input(s)

3.4.9.4 Operational Metrics

A. Total Number Of Applicable IT Security Operational Directives (e.g. Communication Task Orders (CTOs)) Issued
B. Number Of Applicable IT Operational Directives (e.g. Communication Task Orders (CTOs)) Acknowledged Within Timeframe
C. Number Of Applicable IT Operational Directives With a Government Approved POA&M in place
D. Number Of Applicable IT Operational Directives Completed and Reported as Directed
E. Number Of POA&Ms Submitted for Government Approval

3.4.9.5 Key Performance Indicators

3.4.9.5.1 IT Security Operational Directives Acknowledge Rate [Metric: B/A]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.4.9.5.2 IT Security Operational Directives Compliance Rate [Metric: (C+D)/A]

- *Superior Service Threshold: 98%*
- *Service Warning: 90%*

3.4.9.5.3 IT Security Operational Directives POA&M Rate [Metric: (A-D)/E]

- *Superior Service Threshold: 1*
- *Service Warning: >1*

3.4.9.6 Critical Success Factors

- Maintain Mission Assurance with IT Services [KPI: 1, 2, 3]
- Protect and Defend IT Services from Threats [KPI: 2, 3]
- Maintain IT Security Compliance [KPI: 2, 3]

3.4.10 Sub-Task 9: Event Management

3.4.10.1 Overview

Event Management is the process that monitors all events that occur through the NORAD and USNORTHCOM enterprise IT infrastructure to allow for normal operation of facility, network, system, capability, and security services. Event management uses monitoring to detect and escalate exception conditions. Event management extracts information from data being collected that is determined to be of importance for current or future actions, audits or correlations. This process provides notifications created by an IT service, Configuration Item (CI), or monitoring tool that can be programmed to communicate operational information as well as warnings and exceptions, and be used as a basis for automating many operational management activities.

The goal of Event Management is to detect, analyze, and determine course(s) of action for the NORAD and USNORTHCOM enterprise IT infrastructure.

3.4.10.2 Requirements

The Contractor Shall:

3.4.10.2.1 Provide, integrate, and manage Event Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.4.10.2.2 Maximize the use of event management systems to enable monitoring of service assets throughout the enterprise, and assist subordinates and components in their use.

3.4.10.2.3 Tune all monitoring devices to ensure that environmental, network operations, systems operations, service operations, and security operations thresholds provide meaningful and actionable information. Automate responses, actions, and triggers.

3.4.10.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Event Management Report **[CDRL A003]**
2. Event Monitoring Plan

3.4.10.4 Operational Metrics

A. Number Of Monitored Events (Alerts, Informative, Exceptions)
B. Number Of Monitored Events Resulting In Service Desk Recorded Incidents
C. Number Of Repeated Or Duplicated Monitored Events Breaking A Threshold
D. Number Of Each Type Of Monitored Event Per Service Breaking A Threshold
E. Number Of Service Incidents Not Reported By Monitored Events
F. Number Of Monitored Events Requiring Human Intervention
G. Number Of Monitored Events Requiring Human Intervention Not Performed
H. Total Number Of Service Incidents
I. Total Of Services in the Service Catalog
J. Number Of Services with an Event Monitoring Plan

3.4.10.5 Key Performance Metrics

3.4.10.5.1 Event Customer Impact Rate [Metric: (B/A)] *Exclude Informative Events

- *Superior Service Threshold:* 10%
- *Service Warning:* 20%

3.4.10.5.2 Event Repetition Rate [Metric: (C/A)]

- *Superior Service Threshold:* 10%
- *Service Warning:* 20%

3.4.10.5.3 Monitoring Event Effectiveness [Metric: (E/H)]

- *Superior Service Threshold:* 10%
- *Service Warning:* 15%

3.4.10.5.4 Monitored Events Inaction Rate (i.e., Events Where Human Intervention Not Performed) [Metric: (G/F)]

- *Superior Service Threshold:* 2%
- *Service Warning:* 5%

3.4.10.5.5 Service Monitoring Rate [Metric: (D/A)]

- *Superior Service Threshold:* 10%
- *Service Warning:* 20%

3.4.10.5.6 Service Monitoring Plans [Metric: (J/I)]

- *Superior Service Threshold:* 90%
- *Service Warning:* 80%

3.4.10.6 Critical Success Factors

- Optimize overall Mission Risks [KPI: 1, 2, 4, 6]
- Demonstrate and Promote IT Service Efficiency [KPI: 3, 4, 5]
- Minimize User/Customer Impact to IT Service Disruptions [KPI: 1, 2, 6]

3.5 Task 3: Service Strategy Support

3.5.1 Overview

IT Portfolio Management activities begin with customer concepts through chartered service packages to meet the customer's Functional and Service Level Requirements. IT Portfolio Management also includes the maintaining financial, supplier, service level, and service catalog management throughout the lifecycle for all service in the N-NC IT Service Portfolio. The goal of IT Portfolio Management is to achieve value through efficient and effective decision-making about current and future IT investments that support the command's mission.

3.5.2 Sub-Task 1: Service Portfolio Management

3.5.2.1 Overview

Service portfolio describes the services of a provider in terms of NORAD and USNORTHCOM's mission. It articulates mission needs and the service provider's response to those needs and assures that the services provided are measurable with regard to mission accomplishment.

The goal of Service Portfolio Management is to establish and enforce the method for governing investments in IT Service Management.

3.5.2.2 Requirements

The Contractor Shall:

3.5.2.2.1 Provide, Integrate, Execute, and Manage the entire Service Pipeline in the N-NC Service Portfolio, to include third-party managed projects. The contractor will interact directly with all third-party entities (government or other contractor) for project status updates and other Service Portfolio Management activities. Manage the N-NC Service Portfolio for all IT Services from concept through retirement, regardless of Service Provider. At Contract Start the Contractor shall be prepared to take action on all Service Requirements and Projects in the Service Pipeline, see Technical Library for Service Pipeline and Project listing.

3.5.2.2.2 Comply contractor Service Portfolio Management internal processes to integrate and support government Service Portfolio Management processes, to include the C4 Integration Process and Service Portfolio Management Standard Operating Procedures.

3.5.2.2.3 Establish, Manage, and Brief the status of the Service Pipeline. The contractor will provide bi-weekly Service Portfolio status brief to leadership for all services in concept, pipeline, transition, and recommended for retirement.   The Service Portfolio status will also be provided during weekly action-officer meetings between the contractor and the government. Meeting minutes and administrative functions (e.g. scheduling, room and presentation set-up, etc…) will be provided by the contractor for both of these meetings. A real-time work flow tool will be aligned to existing Service Portfolio Management process with Government access to provide insight on day-to-day work. The contractor shall meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.5.2.2.4 Upon Service Request submittal, the Service Desk shall make an immediate assessment of whether a service request is a standard or a non-standard. As such, Service Deck personnel shall have sufficient knowledge and training to know whether a request falls within the realm of a standard or non-standard request upon receipt. The contractor will report (daily) to the government Service Portfolio Manager as to the disposition of new and existing all non-standard service requests in the pipeline. If the non-standard request was submitted by a directorate Customer Representative, the request will be evaluated to determine if it is a candidate to become a standard request and routed to the Change Advisory Board (CAB) for approval. If the submitting party is not a directorate Customer Representative, then the Service Desk will refer the user back to their directorate Customer Representative and close the ticket. The contractor shall analyze and process the disposition of the non-standard service request using the Non Standard Request Analysis Report output specification.   “Analyze and process” means that the nature of the new or significantly modified service is determined, the request description has been updated to reflect the nature of the capability gap and that the Service Request has been forwarded to the appropriate area(s) for action.

3.5.2.2.5 Submit to the Government Service Portfolio Manager, within five (5) business days of user submittal, the Non Standard Request Analysis Report. Exceptions to meeting this timeline shall be formally requested within the same five (5) business days with a justification and an expected delivery date for report completion. The Government will approve/disapprove the exception within 3 business days or the exception timeline is automatically granted. The Contractor shall have the capacity to produce (on average) 35 Non-Standard Analysis Reports per month. No formal government action is required to the

Non-Standard Analysis Report for the Contractor Service Portfolio Management process to continue.

3.5.2.2.6 Schedule, Coordinate, Develop, and Produce a Service Package for each approved Mission Case to enable Command's IT Corporate Board decisions on IT investments and chartering of services. Within 3 days of the approved Mission Case, provide an updated Service Portfolio Delivery Schedule. Each Service Package will be completed within fifteen (15) business days from the date of Mission Case approval; unless additional days are requested and approved by the Government based on complexity, scope, and/or mission need. Exceptions to meeting the specified time must be requested to the Government within the same three (3) business days of the Service Portfolio Delivery Schedule with a justification. The Contractor shall have the capacity to produce ten (10) Service Packages per month. The Contractor should expect that Service Packages will vary in scope and complexity.

3.5.2.2.7 Submit to the Government Service Portfolio Manager, within ten (10) business days after direction by the government, the Investment Analysis Report for all requirements that do not meet corporate investment thresholds. Exceptions to meeting this timeline shall be formally requested within the same ten (10) business days with a justification and an expected delivery date for report completion. The Government will approve/disapprove exception timelines within three (3) business days or the timeline automatically granted. The Contractor shall have the capacity to produce (on average) 25 per month.

3.5.2.2.8 **(Optional Task)** Provide pricing for additional Service Package development above this estimate on a per Service Package basis, these will be executed on the Contractor's proposed price for this task and executed under an optional CLIN.

3.5.2.2.9 **(Optional Task)** Schedule, Coordinate, Develop, and Produce a Mission Case, within 10 (ten) business days, for all requirements that exceed corporate investment thresholds. Within 3 days of the *Non-Standard Analysis Report*, provide an updated *Service Portfolio Delivery Schedule*. This mission case is presented to the Command's Command, Control, Communication, and Computers Integration Process (C4IP) for scoring and prioritization. Coordination shall be performed with the government Business Relationship Manager, directorate Customer Representative and User. Timelines for Mission Case production are solely the responsibility of the contractor. Exceptions to meeting the specified time must be requested to the Government within the same three (3) business days of the Service Portfolio Delivery Schedule with a justification. The Contractor shall have the capacity to produce ten (10) Mission Cases per month.

3.5.2.3 Outputs

See Appendix E Service Output Specifications

1. Monthly Service Portfolio Management Report **[CDRL A003]**
2. **(Optional Task)** Mission Case(s)
3. Service Package(s)
4. Non-Standard Request Analysis Report
5. Investment Analysis Report

3.5.2.4 Operational Metrics

A. Total Number Of Non Standard Service Request Analysis Reports Scheduled
B. Number Of Service Packages Scheduled
C. Number Of Service Packages Completed
D. Number of Non Standard Service Request Analysis Reports Completed
E. Total Number of Investment Analysis Reports Scheduled
F. Number of Investment Analysis Reports Completed

3.5.2.5 Key Performance Indicators

3.5.2.5.1 Monthly Service Package Completion Rate [Metric: C/B]

- *Superior Service Threshold: 98%*
- *Service Warning: 80%*

3.5.2.5.2 Non Standard Service Request Completion Rate [Metric: D/A]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.5.2.5.3 Investment Analysis Report Completion Rate [Metric: F/E]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.5.2.6 Critical Success Factors

- Optimize IT Service Investments [KPI: 1, 3]
- Improve Quality of IT Services [KPI: 1, 3]
- Provide Effective and Efficient IT Service Management [KPI: 2]

3.5.3 Sub-Task 2: ITSM Financial Management

3.5.3.5 Overview

The NORAD and USNORTHCOM Financial Management process incorporates applicable Federal and DoD regulatory guidance. Financial Management is responsible for the oversight of ITSM expenditures needed to ensure efficient and cost effective service delivery.

The goal of ITSM Financial Management is to provide effective stewardship of IT assets and resources used in providing IT services.

3.5.3.6 Requirements

The Contractor Shall:

3.5.3.6.1 Provide, integrate, and support ITSM Financial Management for NORAD and USNORTHCOM in alignment with Government Financial Management process to meet outputs and their associated output specifications, Operational Metrics, Key Performance Indicators and Critical Success Factors identified below.

3.5.3.6.2 Support development of a Lifecycle Technical Refresh Plan for IT Service Assets supporting Services in the Service Catalog. Support future budget analysis and recommendations on service asset upgrades and replacement. Implement Government-approved annual service asset lifecycle replacement decisions.

3.5.3.6.3 Develop an IT budget and spend plan for Government review and approval of the planned ODC expenditures to support pre-approved standard change models, request models, incident models to ensure adequate bench stock is available to meet priority requests and incident response times, and service asset lifecycle replacement.

3.5.3.7 Outputs

See Appendix E Service Output Specifications

1. Monthly ITSM Financial Management Report **[CDRL A003]**
2. Semi-Annual ITSM Budget Forecast Report **[CDRL A010]**
3. Semi-Annual ITSM TCO Report **[CDRL A010]**

3.5.3.8 Operational Metrics

A. Cumulative ITSM Spend Plan (Contractor Controlled Budget, Procurement CLINs)

B. Cumulative ITSM Actual Costs (Contractor Controlled Budget, Procurement CLINs)
C. Number Of Financial Reports/Forecasts Delivered Late
D. Total Number Of Financial Report/Forecasts Delivered
E. Number Of Services In Service Catalog
F. Number Of Services Without A Total Cost of Ownership (TCO) Model
G. Service Design Package Projected Cost
H. Service Design Package Actual Cost

3.5.3.9 Key Performance Metrics

3.5.3.9.1 Cost Performance Variance Index [Metric: ((|B-A|)/A)]

- *Superior Service Threshold:* 2%
- *Service Warning:* 5%

3.5.3.9.2 Financial Reports/Forecasts Delinquency Rate [Metric: C/D]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.5.3.9.3 Service Cost Model Completion Rate [Metric: 1-(F/E)]

- *Superior Service Threshold:* 95%
- *Service Warning:* 85%

3.5.3.9.4 Service Design Package Cost Variance Rate [Metric: ((|H-G|)/G)]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.5.3.10 Critical Success Factors

- Demonstrate and Promote IT Service Efficiency [KPI: 1, 3, 4]
- Provide Effective and Efficient IT Service Management [KPI: 1, 3, 4]
- Improve the Quality of IT Service Management Decisions [KPI: 2, 4]
- Optimize IT Service Investments [KPI: 4]

3.5.4 **(Optional Task) Sub-Task 3: Demand Management**

3.5.4.5 Overview

Demand Management aligns supply with demand and aims to predict demand as closely as possible. This process is primarily responsible for synchronizing consumption (demand) with the capacity (supply) of IT resources in the Service Portfolio. This involves balancing resource capabilities against requests for services and prioritization to address short-term, tactical needs.

The goal of Demand Management is to understand and influence customer demand for services and guide the provision of capacity to meet these demands.

3.5.4.6 Requirements

The Contractor Shall:

3.5.4.6.1 Provide, integrate, and manage Demand Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.5.4.7 Outputs

See Appendix E Service Output Specifications

1. Monthly Demand Management Report **[CDRL A003]**
2. Core Service Packages (CSP)
3. Service Level Packages (SLP)
4. Patterns Of Business Activity (PBA)
5. User Profiles

3.5.4.8 Operational Metrics

A. Number Of Lines Of Service (LOS) In The Service Catalog
B. Number of LOS Without Differentiated Offerings
C. Number Of Services In The Service Catalog
D. Number Of Services Without Documented PBA
E. Number Of Services Without User Profiles
F. Number Of Services Without CSP
G. Number Of Services Without SLP
H. Time Between Updated PBA Analysis Per Service (Months)
I. Number Of Service Packages Scheduled For Review (e.g. User Profiles, CSP, SLP Of Updated PBA)
J. Number Of Service Package Reviews Conducted

3.5.4.9 Key Performance Metrics

3.5.4.9.1 Demand Management Coverage Rate [Metric: 1-(B/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.5.4.9.2 PBA Utilization Rate [Metric: 1-(D/C)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.5.4.9.3 User Profile Utilization Rate [Metric: 1-(E/C)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.5.4.9.4 CSP Utilization Rate [Metric: 1-(F/C)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.5.4.9.5 SLP Utilization Rate [Metric: 1-(G/C)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.5.4.9.6 Time Between Updated PBA Analysis Per LOS (Months) [Metric: H]

- *Superior Service Threshold:* 3 Months
- *Service Warning:* 4 Months

3.5.4.9.7 Service Package Review Rate [Metric: J/I]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.5.4.10 Critical Success Factors

- Maintain a Viable and Accurate IT Environment [KPI: 1, 3, 4, 5, 6]
- Improve Mission/Productivity with IT Services [KPI: 1, 2, 3]
- Improve Quality of IT Services [KPI: 1, 6, 7]

3.5.5 **(Optional Task) Sub-Task 4: IT Enterprise Architecture**

3.5.5.5 Overview

IT Enterprise Architecture supports the development and maintenance of enterprise architectural technical and standards products for the IT Enterprise baseline, target, and vision enterprise architecture models for N-NC mission sets. Supports N-NC critical capabilities, process improvement, and IT portfolio investment strategy.

The IT Enterprise Architecture products will provide a systems-to-mission mapping enabling identification of operational and IT gaps, shortfalls, and duplications that exist in the N-NC enterprise.

3.5.5.6 Requirements

The Contractor Shall:

3.5.5.6.1 Provide, integrate, and manage IT Enterprise Architecture to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.5.5.6.2 Analyze, Develop, Update, and Maintain Baseline Enterprise Architecture per Government Specified Department of Defense Architecture Framework (DODAF) – compliant views.

3.5.5.6.2.1 Analyze existing enterprise architecture technical and standards products and provide recommendations to develop update and maintain baseline architecture products and data for N-NC mission sets and critical processes.

3.5.5.6.2.2 Provide baseline architecture products and maintain updates. The baseline architecture products shall be documented and submitted to the Government within 6 months of the contract start date. Produce architectural products using the current documentation standard, MS Visio.

3.5.5.6.2.3 Assess expected future operational capabilities, and perform system-to-mission mapping to identify operational and IT gaps, shortfalls and duplication that exist in the N-NC enterprise architecture.

3.5.5.6.2.4 Develop and document N-NC vision architecture by analyzing the Command's future capabilities derived from current Joint Operating Concepts, N-NC Strategic Vision, N-NC/J6 Campaign Plan and other relevant mission documents. Perform system-to-mission mapping to identify operational and IT gaps, shortfalls and duplication that exist in the N-NC environment.

3.5.5.6.3 Identify IT capability gaps, shortfalls, or duplication of services and technologies in the N-NC IT Enterprise. Validate submitted IT requirements and projects are aligned with N-NC enterprise architecture.

3.5.5.6.4 Attend and participate in monthly meetings to provide reviews, analysis, and recommendations of IT Enterprise Architectural products and updates.

3.5.5.6.5 Attend and participate in IT Enterprise Architecture Conferences to provide reviews, analysis, and recommendations of IT Enterprise Architectural products and updates.

3.5.5.7 Outputs

1. Quarterly Architecture Products & Updates (**CDRL A007**)
    a. Architecture Diagrams (SvcV-1, SvcV-2, SvcV-6, SvcV-10)
    b. Service Systems Matrix (SvcV-3)

c. Service Functionality Description (SvcV-4)
d. Service Measures Matrix (SvcV-7)
e. Service Evolution Description (SvcV-8)
f. Service Technology & Skills forecast (SvcV-9)

3.5.5.8Operational Metrics

A. Total Number of Services in the Service Catalog
B. Number of Services Not Covered in the Service View Points

3.5.5.9 Key Performance Metrics

3.5.5.9.1 Services View Coverage Rate [Metric: 1-(B/A)]

- *Superior Service Threshold:* 95%
- *Service Warning:* 85%

3.5.5.10 Critical Success Factors

- Maintain a Viable and Accurate IT Environment [KPI: 1]
- Optimize IT Service Investments [KPI: 1]

3.6 Task 4: Service Design

3.6.1 Overview

Service Design activities transition approved and chartered service packages to service design package to meet the customer's intended mission outcomes, Functional Requirements, and Service Level Requirements. The goal of Service Design is to achieve business value through a repeatable service design approach.

3.6.2 Sub-Task 1: Design Coordination

3.6.2.1 Overview

Design Coordination provides a single point of coordination and control for all Service Design lifecycle process activities. It is a critical process for ensuring consistent design principles are applied to the implementation of new and/or significantly changed services.

The goal of Design Coordination is to efficiently and effectively perform the service design processes to meet service charters and change requests for services that are to be transitioned into the NORAD and USNORTHCOM Service Catalog.

3.6.2.2 Requirements

The Contractor Shall:

3.6.2.2.1 Provide, integrate, and manage Design Coordination to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.6.2.2.2 Design and plan to maximize current IT technology and investments in the NORAD and USNORTHCOM environment to meet all customer Functional Requirements (Utility), Service Level Requirements (Warranty), and Service Acceptance Criteria.

3.6.2.2.3 Develop and document Service Design Package(s) for new or changed services and for service assets that require upgrade, modifications, or improvement (e.g. Service Improvement Packages) as part of normal sustainment and industry best practices. Service Design Packages will be coordinated with and presented to the Government for engineering board review and acceptance. The Contractor shall review and participate in engineering review boards for Third-Party produced Service Design Packages.

3.6.2.2.4 Produce Service Design Package(s) within 20 business days from the date of Government Service Package chartering. Schedule Service Design Package completion date within 3 (three) business days from Government Service Package chartering. Exceptions to meeting the specified time must be requested to the Government within the 3 (three) business days of Service Package chartering with a justification and an expected delivery date for Service Design Package completion. The Contractor shall develop Service Design Packages for new and significantly changed services that are not to be developed by a Third-Party. The Contractor shall have the capacity to produce an average of 10 (ten) Service Design Packages per quarter. The Contractor should expect that Service Design Packages will vary in scope and complexity.

3.6.2.2.5 Provide Evaluation Reports and comment resolution feedback to the Government for Third-Party Service Design Packages within 10 (ten) business days of receipt from the Government. Exceptions to meeting the specified time must be requested to the Government within the 3 (three) business days with a justification and an expected delivery date for report completion.

3.6.2.2.6 (Optional Task) Provide pricing for additional Service Design Package development above this estimate on a per Service Design Package basis, these will be executed on the Contractor's proposed price for this task and executed under an option CLIN.

3.6.2.3 Outputs

See Appendix E Service Output Specifications

1. Service Design Package(s)

3.6.2.4 Operational Metrics

A. Total Number Of Scheduled Service Design Packages
B. Number Of Scheduled Service Design Packages Completed

3.6.2.5 Key Performance Metrics

3.6.2.5.1 Service Design Package Completion Rate [Metric: (B/A)]

- *Superior Service Threshold:* 95%
- *Service Warning: 90%*

3.6.2.6 Critical Success Factors

- Implement Quality IT Services [KPI: 1]
- Provide Effective and Efficient IT Service Management [KPI: 1]

3.6.3 Sub-Task 2: Service Level Management

3.6.3.5 Overview

Service Level Management (SLM) represents the IT service provider (N-NC/J6) to the customer (Command ITSM users). SLM monitors and reports on service levels, and manages the expectations of both parties.

The goal of the Service Level Management process is to ensure that an agreed level of IT service is provided for all current NORAD and USNORTHCOM IT services to the Commands ITSM users, and that future services are designed and delivered to agreed achievable targets.

3.6.3.6 Requirements

The Contractor Shall:

3.6.3.6.1 Provide, integrate, and manage Service Level Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.6.3.6.2 Coordinate and draft for Government approval, within 90 days of contract start, Service Level Agreements (SLAs) for all services in the N-NC Service Catalog between N-NC/J6 and each N-NC Headquarters Directorate and Special Staff.

3.6.3.6.3 Coordinate and draft for Government approval, within 90 days of contract start, Operational Level Agreements (OLAs) between N-NC/J6 and the 721st CS; N-NC/J6 and the ODCs; N-NC/J6 and the N-NC Washington Office; and N-NC/J6 and N-NC Subordinate organizations (JTF-CS, JTF-N, JFHQ-NCR, ANR, CONR, CANR); and intra J6 organizations for all services that share technical and application management responsibilities.

3.6.3.7 Outputs

See Appendix E Service Output Specifications

1. Monthly Service Level Management Report **[CDRL A003]**
2. Service Level Agreement(s)
3. Organizational Level Agreement(s)

3.6.3.8 Operational Metrics

A. Number Of Services In The IT Service Catalog

B. Number Of Services In The IT Service Catalog Without SLAs
C. Number Of Supporting Services Delivered By Vendors
D. Number Of Vendor Delivered Services Without Documented SLA In The Underpinning Contract
E. Total Number Of SLA Service Targets
F. Total Number Of SLA Service Targets Breached
G. Number Of Services IT Service Catalog Operating Without Service Owners

3.6.3.9 Key Performance Metrics

3.6.3.9.1 SLA Coverage Rate [Metric: 1-(B/A)]

- *Superior Service Threshold: 95%*
- *Service Warning:* 90%

3.6.3.9.2 Percent Of Vendor Services Delivered Without Documented SLA In The Underpinning Contract [Metric: D/C]

- *Superior Service Threshold: 2%*
- *Service Warning: 10%*

3.6.3.9.3 Percent Of SLA Service Targets Adhered To [Metric: 1-(F/E)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.6.3.9.4 Percent Of SLAs With Assigned Service Owners [Metric: 1-(G/A)]

- *Superior Service Threshold:* 95%
- *Service Warning: 90%*

3.6.3.10 Critical Success Factors

- Optimize User/Customer IT Awareness [KPI: 1, 3]
- Minimize User/Customer Impact to IT Service Disruptions [KPI: 1, 2, 3]
- Provide Effective and Efficient IT Service Management [KPI: 1, 4]
- Maintain Quality IT Services [KPI: 2, 3]

3.6.4 Sub-Task 3: Service Catalog Management

3.6.4.5 Overview

Service Catalog Management provides a single source of accurate, real-time information on all Government approved operational NORAD and USNORTHCOM IT services and service assets provided to the command. The service catalog reflects the current IT environment details, status, interfaces and services in operation and transition.

The goal is the development and maintenance of a published service catalog that contains all accurate details, status, interfaces, interactions, and mutual dependencies of current services.

3.6.4.6 Requirements

The Contractor Shall:

3.6.4.6.1 Provide, integrate, and manage Service Catalog Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.6.4.6.2 Develop, implement, automate, and make available within 90 days of contract start date an unclassified service catalogs that provides both customer and technical catalog views. The customer view shall provide users with accurate content and information for all customer-facing services that can be requested in the N-NC Service Catalog. The technical view links services to service assets and enables the ability to view those relationships.

3.6.4.6.3 Develop Core Service and Service Level Packages for each service in the N-NC Service Catalog within 90 days of contract start date.

3.6.4.7 Outputs

See Appendix E Service Output Specifications

1. Monthly Service Catalog Report **[CDRL A003]**
2. Published Portal-based Service Catalog
3. Core Service Package(s)
4. Service Level Package(s)

3.6.4.8 Operational Metrics

A. Number Of Differentiated Offerings (Service Level Packages) In Service Catalog
B. Time Between Service Audits (list services, with last audit performed)
C. Number Of Services Level Packages Without Complete Service Packages, to include Core Service Package and Service Level Package(s)

3.6.4.9 Key Performance Metrics

3.6.4.9.1 Time Between Service Audits. Metric: [B]

- *Superior Service Threshold:* 90 days
- *Service Warning:* 120 days

3.6.4.9.2 IT Service Catalog Completeness Ratio. Metric: [1-(C/A)]

- *Superior Service Threshold: 98%*
- *Service Warning: 95%*

3.6.4.10 Critical Success Factors

- Maintain a Viable and Accurate IT Environment [KPI: 1]
- Optimize User/Customer IT Awareness [KPI: 1]
- Demonstrate and Promote IT Service Efficiency [KPI: 1, 2]

3.6.5 Sub-Task 4: Supplier Management

3.6.5.5 Overview

The NORAD and USNORTHCOM Supplier Management process incorporates applicable Federal and DoD regulatory guidance. Supplier Management is responsible for the acquisition of supplies and services to support NORAD and USNORTHCOM ITSM service targets.

The goal of the Supplier Management is to manage suppliers and the services they supply to provide IT service in accordance with agreed upon service targets (e.g., SLAs and OLAs).

3.6.5.6 Requirements

The Contractor Shall:

3.6.5.6.1 Provide, integrate, and manage Supplier Management in alignment with the Government Supplier Management policy and process to meet outputs and their associated specifications, Operational Metrics, Key Performance Indicators and Critical Success Factors identified below.

3.6.5.6.2 Review and analyze all underpinning contracts; provide recommendations to the Government on renewal, modification, and/or allow expiration at least 150 days prior to contract expiration.

3.6.5.6.3 Provide complete procurement packages for all underpinning contracts 60 days prior to contract expiration.

3.6.5.6.4 Procure all IT service assets required for incidents, standard service requests, and service asset lifecycle replacement.

3.6.5.6.5 Review all underpinning contracts annually by the end of 2nd Quarter of the Fiscal Year for preparation towards the follow-on fiscal year spend planning for maintenance and warranty agreements.

3.6.5.6.6 Survey all Underpinning Contracts monthly to identify usage of the agreement to support service level agreements, warranties, or escalated maintenance.

3.6.5.7 Outputs

See Appendix E Output Specifications

1. Monthly Supplier Management Report **[CDRL A003]**
2. Procurement Package(s)
3. Underpinning Contract Recommendation(s)

3.6.5.8 Operational Metrics

A. Total Number Of Supplier Management Reports Delivered
B. Number Of Supplier Management Reports Delivered Late
C. Total Number Of Service Level Agreements
D. Number Of SLAs Breached Due To Inadequate Underpinning Contract(s)
E. Number Of Underpinning Contracts within 180 calendar days of expiration
F. Number of Underpinning Contracts within 180 calendar days of expiration and not validated
G. Number of Validated Underpinning Contracts within 150 calendar days of expiration
H. Number of Underpinning Contract recommendations submitted on Validated Underpinning Contracts within 150 calendar days of expiration
I. Total Number Of Procurement Packages Submitted
J. Number Of Procurement Packages Forecasted
K. Number Of Incomplete Procurement Packages Submitted
L. Total Number of Underpinning Contracts
M. Number of Underpinning Contracts Surveyed for Use
N. Number of Underpinning Contracts within 60 days of expiration
O. Number of Underpinning Contract Procurement Packages Submitted

3.6.5.9 Key Performance Metrics

3.6.5.9.1 Percentage Of Late Supplier Management Reports. [Metric: B/A]]

- *Superior Service Threshold:* 2%
- *Service Warning:* 5%

3.6.5.9.2 Percentage Of Underpinning Contract SLAs Breaches. [Metric: (1-(D/C))]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.5.9.3 Underpinning Contract Validation Rate. [Metric: (1-F/E)]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.5.9.4 Underpinning Contract Submission Rate. [Metric: (1-(H/G))]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.5.9.5 Procurement Package Submission Rate. [Metric: (J/I)]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.5.9.6 Procurement Package Accuracy Rate. [Metric: (1-(K/I))]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.5.9.7 Underpinning Contract Surveillance Audit Rate. [Metric: (M/L)

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.5.9.8 Underpinning Contract Procurement Package Rate. [Metric: (O/N)

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.6.5.10 Critical Success Factors

- Maintain Quality IT Services [KPI: 2, 4, 5, 7, 8]
- Improve the Quality of IT Service Management Decisions [KPI: 3, 4, 5, 6, 7, 8]
- Deliver Accurate and Timely IT Services [KPI: 1, 2]

3.6.6 Sub-Task 5: Information Security Management

3.6.6.5 Overview

The NORAD and USNORTHCOM Information Security Management (ISM) process incorporates all applicable policies and regulations and seeks to ensure that information security is effectively incorporated in all service and service management activities related to the confidentiality, integrity, availability, authentication and non-repudiation of information systems and data to include the security of hardware and software components, documentation and security procedures across the enterprise which includes the NNC owned circuits, NNC domains and NNC IP ranges. The ISM Government process develops and enforces policy, standards, and procedures to ensure the protection of the organization's assets, data, information, and IT services.

The goal of ISM is to align IT and mission security to ensure that information security is employed effectively in all NORAD and USNORTHCOM IT services and service management activities in accordance with applicable legal and regulatory guidance and organizational policy.

The overarching governance for the ISM requirements is captured in, but is not limited to, references included in Appendix A – Publications and Appendix E – Output Specifications. The Contractor will maintain awareness of all applicable Government policy, standards, mandates, and regulations as they apply to IT security. The governance outlines regulatory requirements to be used by the Contractor to ensure the NORAD and USNORTHCOM enterprise (e.g. systems and networks) are in compliance and are inspection ready at all times.

3.6.6.6 Requirements

The Contractor Shall:

3.6.6.6.1 Provide, integrate, and manage Information Security Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate compliancy with required security governance.

3.6.6.6.2 Install, operate, maintain, troubleshoot, and upgrade boundary protection systems to include, but not limited to: firewalls, intrusion detection/prevention systems, patch management, web proxies, and external routers. The Contractor shall maintain and manage Information Assurance vulnerability compliance through Government-designated tools (e.g. Vulnerability Management System (VMS), Host Based Security System (HBSS)).

3.6.6.6.3 Comply with all DISA Security Technical Implementation Guides (STIGs) (e.g. network STIG, enclave STIG, non-traditional STIG) for all service assets in the N-NC Service Catalog.

3.6.6.6.4 Anticipate and plan for near-term changes in the DISA and USCYBERCOM information assurance requirements for vulnerability management, scanning, and compliance capabilities that may replace and/or retire current information assurance and security capabilities.

3.6.6.6.5 Provide the following items to be used by the Government for validation and acceptance for compliance of information assurance and security requirements:

3.6.6.6.5.1 IA Controls – Provide IA Control report bi-annually to include at a minimum compliant controls, detailed non-compliant controls (must be approved by the Government), plans of actions and milestones (POA&Ms) for mitigation of non-compliant controls, planned completion dates and applicable N-NC network/system Mission Assurance Category (MAC) and Classification Levels.

3.6.6.6.5.2 DOD Designated Vulnerability Tracking System – Manage and maintain general asset and scan entries in Government-designated system to include at a minimum, but not limited, to scans, Security Technical Implementation Guide (STIGs), Government approved POA&Ms as directed by Government (e.g. CJCSI 6510, CTO 08-005, N-NC, DISA, USCYBERCOM directives).

3.6.6.6.5.3 Vulnerability Scans –Scan and identify vulnerabilities within the boundaries of the N-NC Service Catalog. (e.g. CJCSI 6510, CTO 08-005, N-NC, DISA, USCYBERCOM directives).

3.6.6.6.5.4 Patch Systems – Maintain knowledge of required patches and deploy as specified by directives and tasking orders. At a minimum, identify systems out of compliance and patch/reimage accordingly. If a network or system is provided by a Third-Party the Contractor will notify the supporting organization of other network or system non-compliance and track until completion. Patches older than 30 days must be corrected or have a valid Government approved POA&M and be tracked within the Government-designated system (e.g. VMS). Zero-day vulnerabilities will be tracked and corrected as soon as the applicable patch becomes available. Mitigation to protect from zero-day vulnerabilities will be provided while awaiting corrective patch (e.g. disable application until patch approved, disable port/protocol).

3.6.6.6.5.5 Ports and Protocols – Manage and maintain ports and protocols to ensure security. Contractor will maintain information that at a minimum includes collected ports and protocols data, vulnerability assessment, assurance category, threat potential to cause damage to DOD operations and interests, a detailed description of exceptions and why necessary, description of the compensating controls in place to mitigate risk, business Impact and Risk, and Threat and Vulnerability Analysis. Ports and Protocols information will be maintained in the Government-designated system (e.g. DOD Ports Protocols and Service Management (PPSM) Registry). The contractor will prepare Technical Review Spreadsheets for all systems requiring port openings when services are not listed in the PPSM registry.

3.6.6.6.5.6 Certification and Accreditation – Provide complete certification and accreditation documentation for new systems and existing systems requiring re-accreditation such as servers, router(s), infrastructure, DISN video services, devices/equipment for new and existing systems that include at a minimum STIG review and findings, applicable manual and/or automated Gold Disk Sessions, Security Readiness Review checklists, vulnerability scans, IA controls, risk assessment to include business impact, scorecard, Government approved POA&Ms and other documentation as required per DOD guidance and N-NC IA Office. Reports should be provided to N-NC IA Office with a minimum of 20 days prior to accreditation approval expectation and system implementation to allow for validation, questions, re-work, boards and final approval to connect by the Authorizing Official (e.g. Designated Accrediting Authority). Adjusted timelines for delivery or review of reports through N-NC IA Office may be necessary.

3.6.6.6.5.7 Command Cyber Readiness Inspection – Manage and maintain security posture and compliance within the N2ITSM boundaries in accordance with DOD inspection criteria. Provide bi-annual status report that includes at a minimum non-compliant items that affect the inspection ready state (satisfactory or better) of the N2ITSM boundaries. .

3.6.6.6.5.8 Circuit and Cross Domain Solution Support – Comply with the DISA Connection Approval Process guidelines, instructions and DOD guidance to manage, maintain, and accredit N-NC Command Communication Service Designators (CCSDs) and Cross Domain Solutions for the N-NC Enterprise. Provide accurate and complete documentation as required for new circuit requests or renewals to include at a minimum circuit details (e.g., IP range, POP address), topologies and SIPRNet Connection Questionnaire. Provide ISP Waiver packages as required to include at a minimum a brief for the Office of Secretary of Defense (OSD) GIG Panel, justification explaining the requirement, technical details, and topology. Provide mitigation actions/activities as required to address findings annotated during remote vulnerability scans and remote compliance assessment scans to address at a minimum CAT 1 findings fixed/mitigated within 30 days of notification. Provide technical reports as required for new and existing Cross Domain requirements. Reports and required documentation will include at a minimum configuration details (e.g., data types, security levels, throughput, topology) and completed Cross Domain template for all four Phases of the Secret and Below Information (SABI) process. Provide report at least annually on Cross Domain configurations and associated POA&Ms for all N-NC cross domain devices. Provide Joint Vulnerability Assessment Process (JVAP) annually.

3.6.6.6.5.9 External Scans-- Comply with all required actions from USCYBERCOM CTO 07-09, Support Remote Vulnerability Assessment and Compliance Monitoring Scans of SIPRNET Enclaves. The Classified Connection Approval Office will conduct announced and unannounced Remote Information Assurance Compliance Assessment Scans of N-NC CCSDs. The contractor will provide support and correct any found discrepancies such as improper firewall settings and identified CAT 1, CAT 2 and CAT 3 discrepancies. CAT 1 weaknesses will be corrected with 15 days, CAT 2 weaknesses corrected within 45 days, CAT 3 weaknesses corrected as directed by the DAA and results provided to the Command Information Assurance Office. Any weakness not corrected in given timeframe will be mitigated and a Plan of Action and Milestone provided.

3.6.6.7 Outputs

See Appendix E Output Specifications

1. Monthly Information Security Management Report **[CDRL A003]**
2. Plan of Actions and Milestones (POA&M)
3. Certification and Accreditation Package(s)
4. Circuit Request(s)
5. Cross Domain Request(s)
6. Technical Review Sheet(s)
7. Quarterly Information Security Management Report **[CDRL A006]**

3.6.6.8 Operational Metrics

A. Number of Unique CAT 1 STIG Compliance Audit Checks Evaluated Per Service
   1) Per NIPR
   2) Per SIPR/SIPR-REL
   3) Per NEN

B. Number of Unique CAT 2 STIG Compliance Audit Checks Evaluated Per Service
   1) Per NIPR
   2) Per SIPR/SIPR-REL
   3) Per NEN

C. Number of Unique CAT 3 STIG Compliance Audit Checks Evaluated Per Service
   1) Per NIPR
   2) Per SIPR/SIPR-REL
   3) Per NEN

D. Number of Unique Failed CAT 1 STIG Compliance Audit Checks Per Service Evaluated without a Government approved POA&M
   1) Per NIPR
   2) Per SIPR/SIPR-REL
   3) Per NEN

E. Number of Unique Failed CAT 2 STIG Compliance Audit Checks Per Service Evaluated without a Government approved POA&M
   1) Per NIPR
   2) Per SIPR/SIPR-REL
   3) Per NEN

F. Number of Unique Failed CAT 3 STIG Compliance Audit Checks Per Service Evaluated without a Government approved POA&M
   1) Per NIPR
   2) Per SIPR/SIPR-REL
   3) Per NEN

G. Total Number of Network Assets Within Scan Range(e.g. Desktops, Laptops, Tablets)
   1) per NIPR
   2) per SIPR/SIPR REL
   3) per NEN

H. Total Number of Network Assets Scanned per Network
   1) per NIPR
   2) per SIPR/SIPR-REL
   3) Per NEN

I. Number of Open CAT 1 Vulnerabilities identified by Scan (Over 30 days since issue date; With No Government approved POA&Ms)
   1) per NIPR

J. Number of Open CAT 2 Vulnerabilities identified by Scan (Over 30 days since issue date; With No Government approved POA&Ms)
   1) per NIPR

K. Number of Open CAT 3 Vulnerabilities identified by Scan (Over 30 days since issue date; With No Government approved POA&Ms)
   1) per NIPR

L. Total Number of Applicable Patches/Security Updates Issued
   1) per SIPR/SIPR-REL
   2) per NEN

M. Total Number of Successful Patches/Security Updates Deployed to Workstations
   1) per SIPR/SIPR-REL
   2) per NEN

N. Number of Number of systems with more than 5 (five) CAT 1 Vulnerabilities
   1) per NIPR

O. Number of Network Assets Within Scan Range (e.g. Desktops, Laptops, Tablets) with all HBSS point products installed in accordance with FRAGO 13 to OPORDER 05-01 or current DoD Directive
   1) per NIPR
   2) per SIPR
   3) Per NEN

3.6.6.9 Key Performance Indicators

3.6.6.9.1 STIG CAT 1 Audit Failure Ratio [Metric: D/A]

1) per NIPR
2) per SIPR/SIPR-REL
3) per NEN

- *Superior Service Threshold: <10%*
- *Service Warning: >20%*

3.6.6.9.2 STIG CAT 2 Audit Failure Ratio [Metric: E/B]

1) per NIPR
2) per SIPR/SIPR-REL
3) per NEN

- *Superior Service Threshold: <10%*
- *Service Warning: >20%*

3.6.6.9.3 STIG CAT 3 Audit Failure Ratio [Metric: F/C]

1) per NIPR
2) per SIPR/SIPR-REL
3) per NEN

- *Superior Service Threshold: <10%*

- *Service Warning: >20%*

3.6.6.9.4 CAT 1 Vulnerability Rate [Metric: I/H]

1) per NIPR

- *Superior Service Threshold: <2.5*
- *Service Warning: >3.5*

3.6.6.9.5 CAT 2 Vulnerability Rate [Metric: J/H]

1) per NIPR

- *Superior Service Threshold: <5.0*
- *Service Warning: >8.0*

3.6.6.9.6 CAT 3 Vulnerability Rate [Metric: K/H]

1) per NIPR

- *Superior Service Threshold: <5.0*
- *Service Warning: >8.0*

3.6.6.9.7 Vulnerability Scan Quality [Metric: [H/G]

1) per NIPR
2) per SIPR/SIPR-REL
3) per NEN

- *Superior Service Threshold: >95%*
- *Service Warning: <90%*

3.6.6.9.8 HBSS Asset Coverage Rate [Metric: O/G]

1) per NIPR
2) per SIPR
3) per NEN

- *Superior Service Threshold: >98%*
- *Service Warning: <95%*

3.6.6.9.9 Security Patch Compliancy Rate [Metric: 1 - (N/H)]

1) per NIPR

- *Superior Service Threshold: >95%*
- *Service Warning: <90%*

3.6.6.9.10 Workstation Patch Compliance Rate [Metric: M/L)

1) per SIPR/SIPR-REL
2) per NEN

- *Superior Service Threshold: >95%*
- *Service Warning: <90%*

3.6.6.10 Critical Success Factors

- Maintain IT Security Compliance [KPI: 1, 2, 3, 4, 5, 7]
- Optimize Overall Mission Risks [KPI: 1, 2, 3, 4, 5 6, 8, 9, 10, 11]
- Maintain Mission Assurance with IT Services [KPI: 1, 2, 3, 4, 5 9, 10]
- Protect and Defend IT Services from Threats [KPI: 1, 9, 10, 11]

3.6.7 **Sub-Task 6: Availability Management**

3.6.7.5 Overview

Availability Management includes designing, implementing, measuring, managing, and improving NORAD and USNORTHCOM IT services and related components' availability. It ensures all services and components are designed and delivered in order to meet their targets in terms of operational and mission need.

The goal of Availability Management is to ensure that the level of service availability delivered in all services meets or exceeds the current and future needs of NORAD and USNORTHCOM in a cost effective manner.

3.6.7.6 Requirements

The Contractor Shall:

3.6.7.6.1 Provide, integrate, and manage Availability Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.6.7.6.2 Analyze and determine supporting technology per service in the N-NC Service Catalog to establish service level targets for availability as currently configured in the N-NC environment within 60 days of contract start.

3.6.7.6.3 Meet and report monthly the Availability service level targets for all core service packages and service level packages in the N-NC Service Catalog.

3.6.7.6.4 Provide Availability Management Plan(s) that details how services in the N-NC Service Catalog are modeled, and how availability is calculated, measured, monitored, and reported with real-time automated sensing tools. The Availability Management Plan(s) will be delivered within 60 days of contract start.

3.6.7.7 Outputs

See Appendix E Output Specifications

1. Monthly Availability Management Report **[CDRL A003]**
2. Availability Management Plan(s)

3.6.7.8 Operational Metrics

A. Total Number Of Incidents
B. Total Number Of OLAs From Internal Suppliers
C. Total Number Of Underpinning Contracts From Vendor Suppliers
D. Number Of Internal OLAs Breached
E. Number Of Vendor Underpinning Contracts Breached
F. Number Of Service Level Targets Missed (per Service)
G. Number Of IT Service Assets Not Supported By Vendors
H. Total Number Of Services In Service Catalog
I. Number Of Services Not Covered By An Active Availability Plan
J. Number Of Services Without Availability Review Last 3 Months
K. Planned Maintenance Time (Hours)
L. Actual Maintenance Time (Hours)

3.6.7.9 Key Performance Indicators

3.6.7.9.1 Average Internal Supplier Service Reliability Index [Metric: 1-(D/B)]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.7.9.2 Average Vendor Supplier Service Reliability Index [Metric: 1-(E/C)]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.7.9.3 Availability Service Level Targets Index [Metric: F/H]

- *Superior Service Threshold: 10%*
- *Service Warning:* 15%

3.6.7.9.4 Availability Risk Index [Metric: I/H]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.6.7.9.5 Continuous Availability Improvement Index [Metric: 1-(J/H)]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.6.7.9.6 Maintenance Window Accuracy Rate [Metric: ((|K-L|)/K)]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.6.7.10 Critical Success Factors

- Improve Mission/Business Productivity with IT Services [KPI: 2, 3]
- Improve Quality of IT Services [KPI: 3, 4, 5]
- Minimize User/Customer Impact to IT Service Disruptions [KPI: 1, 2, 5, 6]

3.6.8 **Sub-Task 7: Capacity Management**

3.6.8.5 Overview

Capacity Management is the discipline that ensures IT infrastructure is provided at the right time in the right volume at the right price, and ensuring that IT is used in the most efficient manner. Capacity Management is responsible for planning and scheduling IT resources to provide a consistent level that matches the current and future requirements of the customer, and balancing cost against resources needed and balancing supply against demand. As such, it is the focal point for all NORAD and USNORTHCOM IT enterprise performance and capacity issues. Capacity Management also considers physical space planning and environmental systems capacity.

The goal of Capacity Management is to ensure that cost-justifiable IT capacity in all areas of NORAD and USNORTHCOM ITSM is matched to the current and future requirements of the business/mission in a timely manner.

3.6.8.6 Requirements

The Contractor Shall:

3.6.8.6.1 Provide, integrate, and manage Capacity Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.6.8.6.2 Analyze and determine supporting technology per service in the N-NC Service Catalog to establish service level targets for capacity as currently configured in the N-NC environment within 60 days of contract start.

3.6.8.6.3 Meet and report monthly the Capacity service level targets for all core service packages and service level packages in the N-NC Service Catalog.

3.6.8.6.4 Provide Capacity Management Plan(s) that details how services in the N-NC Service Catalog are modeled, and how capacity is calculated, measured, monitored, and reported with real-time automated sensing tools. The Capacity Management Plan(s) will be delivered within 60 days of contract start.

3.6.8.7 Outputs

See Appendix E Output Specifications

1. Monthly Capacity Management Report **[CDRL A003]**
2. Capacity Management Plan(s)
3. Quarterly IT Service Utilization Reports **[CDRL A008]**

3.6.8.8 Operational Metrics

A. Total Number Of Services in the Service Catalog
B. Number Of Services Not Covered By An Active Capacity Plan
C. Number Of Services With Capacity Monitoring
D. Total Number of Services Assets w/Component Capacity Monitoring Capability
E. Number Of Incidents Caused By Inadequate Capacity
F. Total Number Of Incidents

3.6.8.9 Key Performance Indicators

3.6.8.9.1 Capacity Risk Index [Metric: B/A]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.6.8.9.2 Service Asset Capacity Monitoring Rate [Metric: C/D]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.6.8.9.3 Inadequate Capacity User Impact [Metric: E/F]

- *Superior Service Threshold:* 2%
- *Service Warning:* 5%

3.6.8.10 Critical Success Factors

- Improve Quality of IT Services [KPI: 2, 3]
- Minimize User/Customer Impact to IT Service Disruptions [KPI: 3]
- Demonstrate and Promote IT Service Efficiency [KPI: 1, 2, 3]

3.6.9 Sub-Task 8: IT Service Continuity Management

3.6.9.5 Overview

IT Service Continuity Management (ITSCM) focuses on the ability to provide continuous IT services to include real-world events and exercises.

The goal of ITSCM is to support the NORAD and USNORTHCOM continuity process by ensuring that the mission essential IT service assets (e.g. computer systems, networks, applications, data repositories, telecommunications, technical support) can be resumed within required timelines.

3.6.9.6 Requirements

The Contractor Shall:

3.6.9.6.1 Provide, integrate, and manage IT Service Continuity Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.6.9.6.2 Analyze and determine supporting technology per service in the N-NC Service Catalog to establish a service level targets for continuity as currently configured in the N-NC environment within 60 days of contract start.

3.6.9.6.3 Provide IT Service Continuity Management Plan(s) that details how services in the N-NC Service Catalog are protected to ensure continuous operations and disaster recovery, and how service continuity is designed, planned, tested, and reported. The IT Service Continuity Management Plan(s) will be delivered within 60 days of contract start.

3.6.9.6.4 Conduct, at a minimum, 2 (two) full IT Service Continuity tests per year. Additionally, be prepared to exercise IT Service Continuity Plan(s) in conjunction with N-NC major exercises.

3.6.9.7 Outputs

See Appendix E Output Specifications

1. Monthly IT Service Continuity Report **[CDRL A003]**
2. IT Services Mission Impact Analysis **[CDRL A012]**
3. IT Service Continuity Plan(s)
4. Quarterly IT Service Continuity Test & Audit Schedule **[CDRL A009]**
5. Quarterly IT Service Continuity Test & Audit Report **[CDRL A009]**

3.6.9.8 Operational Metrics

A. Number Of Services In Service Catalog
B. Number of Services Covered By IT Service Continuity Plans
C. Number of Service Continuity Plan Audit Failures
D. Mean Time (Months) Between Continuity Tests For Each Service
E. Number of IT Services Tested For Service Continuity
F. Mean Time (Months) Between Continuity Plan Audits For Each Service
G. Number Of Services With Test Failures
H. Total Number Of Services Needed To Support ITSCM Plans
I. Number Of Required Internal Support Services Without An OLA
J. Number Of Required External Support Services Without Formal Agreements
K. Number Of IT Service Continuity Plan Audits Conducted

3.6.9.9 Key Performance Indicators

3.6.9.9.1 ITSCM Coverage Ratio [Metric: B/A]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.9.9.2 IT Service Continuity Plan Audit Failure Ratio [Metric: C/K]

- *Superior Service Threshold:* 10%
- *Service Warning:* 20%

3.6.9.9.3 Mean Time (Months) Between Continuity Tests For Each Service [Metric: D]

- *Superior Service Threshold:* 6 Months
- *Service Warning:* 9 Months

3.6.9.9.4 Testing Completeness Ratio [Metric: E/A]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.6.9.9.5 IT Service Continuity Recovery Test Success Rate [Metric: 1-(G/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.6.9.9.6 Mean Time Between Continuity Plan Audits For Each Service [Metric: F]

- *Superior Service Threshold:* 3 Months
- *Service Warning:* 6 Months

3.6.9.9.7 ITSCM Support Service Coverage Ratio [Metric: 1-((I+J)/H)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.6.9.10 Critical Success Factors

- Improve Mission/Business Productivity with IT Services [KPI: 1, 2]
- Improve Quality of IT Services [KPI: 2, 3, 6, 7]
- Minimize User/Customer Impact to IT Service Disruptions [KPI: 2, 3, 4]
- Maintain Mission Assurance with IT Services [KPI: 1, 5, 6, 7]

3.7 Task 5: Service Transition

3.7.2 Overview

Service Transition activities transition approved concepts and chartered service packages to an operational capability to meet the customer's Functional and Service Level Requirements. The goal of Service Transition is to achieve business value through a repeatable service transition planning and support approach.

3.7.3 Sub-Task 1: Transition Planning and Support

3.7.2.1 Overview

Transition Planning and Support is the process responsible for the overall planning and execution of a service through the Service Transition lifecycle. This process provides an integrated approach that aligns service transition plans with customer and service provider mission changes and business project plans.

The goal of Transition Planning and Support is too efficiently and effectively transition services from service design into service operations while realizing and meeting customer value.

3.7.3.2 Requirements

The Contractor Shall:

3.7.3.2.1 Provide, integrate, and manage Transition Planning and Support to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.3.2.2 Responsible for service transition activities (e.g., build, evaluation, tests, release, early life support) until customer acceptance is achieved. This requires that service operations accepts the service and the customer validates all requirements have been met.

3.7.3.2.3 Provide weekly Project Brief covering new or changed service change and projects that the Contractor is responsible. The Project Brief will be updated and presented weekly to the Government Service Owner and management during the Portfolio/Project Update Brief and posted on a portal-based site. The Project Brief input will provide at a minimum project cost, schedule, and performance status.

3.7.3.2.4 Ensure that all Contractor or Third-Party services in transition are planned and coordinated for successful operations by developing an Early Life Support Package for each service in transition. Early Life

Support Package will be developed within 15 business days after the Government approves the Contractor's or Third-Party Release and Deployment Package.

3.7.3.3 Outputs

See Appendix E Output Specifications

1. Project Brief Input(s)
2. Early Life Support Package(s)

3.7.3.4 Operational Metrics

A. Total Changes Implemented Per Month
B. Number Of Changes Resulting In Incidents
C. Total Number of Planned Releases
D. Total Releases Implemented IAW Release Date
E. Number Of Releases Resulting In Incidents
F. Number Of Incidents Caused By New Release (In Service Operations)
G. Total Number Of Release Packages Tests
H. Total Number of Services/Projects in Transition
I. Number of Transition Brief(s) Provided (Weekly)
J. Total Number of Service Design Package(s) Approved by Government
K. Number of Early Life Support Packages Delivered

3.7.3.5 Key Performance Indicators

3.7.3.5.1 Change Incident Rate [Metric: B/A]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.7.3.5.2 Release Defect Rate [Metric: E/D]

- *Superior Service Threshold:* 20%
- *Service Warning:* 30%

3.7.3.5.3 Percentage Of Failed Release Package Tests [Metric: F/G]

- *Superior Service Threshold:* 10%
- *Service Warning:* 15%

3.7.3.5.4 Transition Brief Coverage Rate [Metric: I/H]

- *Superior Service Threshold:* 100%
- *Service Warning:* 90%

3.7.3.5.5 Early Life Support Package Coverage Rate [Metric: K/J]

- *Superior Service Threshold:* 100%
- *Service Warning:* 90%

3.7.3.5.6 Release Timeliness Calculation: [Metric: D/C]

- *Superior Service Threshold:* 90%
- *Service Warning:* 80%

3.7.3.6 Critical Success Factors

- Implement Quality IT Services [KPI: 1, 2, 3,]
- Deliver Accurate and Timely IT Services [KPI 2, 3]
- Provide Effective and Efficient IT Service Management [KPI: 4, 5, 6]

3.7.4 **Sub-Task 2: Change Management**

3.7.4.5 Overview

Change Management is the process responsible for controlling the lifecycle of all changes. Change management ensures that standardized methods and procedures are used for efficient and prompt handling of all changes with minimal disruption to IT Services. Change Management ensures that changes are authorized, recorded, prioritized, planned, tested, implemented, assessed, documented and reviewed in a controlled manner.

The goals of change management are to provide a deliberate response to RFCs in a timely manner.

3.7.4.6 Requirements

The Contractor Shall:

3.7.4.6.1 Provide, integrate, and manage Change Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.4.6.2 Ensure that all Request for Changes (RFC) to any Service, Network, Infrastructure, or supporting systems are submitted to the Government Change Advisory Board (CAB) for approval prior to implementation and/or execution. Obtain Government CAB approval to all non-emergency Request for Change(s) to a minimum of 10 business days prior to start of change implementation. Estimate approximately 150 RFCs produced per month.

3.7.4.6.3 Perform all required activities to coordinate and obtain an Approved Service Interruption (ASI) prior to change implementation.

3.7.4.6.4 Produce standard change models for, at a minimum, O&M activities that are low impact and/or routine within 60 days of contract start. Review existing standard change models and submit to CAB within 60 days of contract start for re-approval; review annually all standard change models thereafter.

3.7.4.7 Outputs

See Appendix E Output Specifications

1. Monthly Change Management Report **[CDRL A003]**
2. Forward Schedule Of Changes
3. Request for Change(s)
4. Standard Change Model(s)

3.7.4.8 Operational Metrics

A. Total Changes In Pipeline Scheduled Per Month
B. Total Changes Implemented Per Month
C. Number Of Failed Changes Per Month
D. Number Of Unauthorized Changes Detected Per Month
E. Number Of Changes Rescheduled Per Month

3.7.4.9 Key Performance Indicators

3.7.4.9.1 Monthly Change Efficiency Rate [Metric: B/A]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.7.4.9.2 Change Success Rate [Metric: 1-(C/B)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.7.4.9.3 Change Reschedule Rate [Metric: E/A]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.7.4.9.4 Unauthorized Change Rate [Metric: D/B]

- *Superior Service Threshold:* 1%
- *Service Warning:* 2%

3.7.4.10 Critical Success Factors

- Implement Quality IT Services [KPI: 1, 2, 3]
- Optimize Overall Mission Risks [KPI: 2, 3, 4]
- Deliver Accurate and Timely IT Services [KPI: 2, 3]

3.7.5 **Sub-Task 3: Service Asset and Configuration Management**

3.7.5.5 Overview

Service Asset and Configuration Management (SACM) ensures that components (Configuration Items) forming delivered services are identified, baselined, and maintained on both the operational network and in the definitive hardware store. It ensures service release into controlled environments and operational use are based on formal approval. SACM provides a logical model of the NORAD and USNORTHCOM ITSM enterprise and maintains accurate configuration information on its historical, planned, and current state.

The goal of SACM is to define and control the components of services to maintain accurate configuration information on their historical, planned, and current states.

3.7.5.6 Requirements

The Contractor Shall:

3.7.5.6.1 Provide, integrate, and manage Service Asset and Configuration Management (SACM) to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.5.6.2 Perform Equipment Control Officer (ECO) duties for all assigned equipment listed in the assigned Defense Reporting Activity. (DRA) Perform all duties and responsibilities IAW AFMAN 33-153 to include but not limited to Service Asset accounting, inventory, reconciliation and sanitization in addition to the training and auditing of ITEC account holders under the USNORTHCOM Defense Reporting Activity (DRA). Manage and maintain the NORAD and USNORTHCOM Equipment Control Officer (ECO) Program IAW governance listed the Technical Library to include but not limited to the receipt, transport, and retirement of Service Assets. The Contractor shall maintain Service Asset records in the Asset Inventory Management (AIM) database.

3.7.5.6.3 Perform Information Technology Equipment Custodian (ITEC) duties IAW AFMAN 33-153 for the NORAD and USNORTHCOM infrastructure and all other ADPE Service Assets used by the Contractor to perform the responsibilities of this PWS.

3.7.5.6.4 Maintain warehouse and storage space IAW industry standards. Comply with all safety requirements IAW industry standards. Perform warehouse, storage, and service asset shipping/receiving functions; store, inventory, package, ship, receive and deliver classified and unclassified ADPE service assets to provision and/or retire services in the N-NC Service Catalog and those services provided to deployed and subordinate organizations. Receive assets and coordinate delivery of assets with Government personnel. Identify and report any damaged or lost items to the Equipment Custodian Officer (ECO). Coordinate Return Merchandise Authorization (RMA) requests with vendors. Complete the Automated Data Processing Equipment (ADPE) AFEMS-AIM accountability paperwork IAW Air Force Manual 33-153 and coordinate completed copies between the ITECs and ECO. Perform hardware relocation between HQ N-NC facilities.

3.7.5.6.5 Schedule and transfer equipment to Defense Reutilization Management Office (DRMO) to ensure timely and efficient turn-in of service assets that are retired or disposed. Service Assets should be scheduled for turn-in with 60 days of retirement.

3.7.5.6.6 Develop and maintain a relational Configuration Management Database (CMDB) which is the sole, trusted source of Configuration Item (CI) data for the NORAD and USNORTHCOM networks.

3.7.5.6.7 Capture, maintain, and update configuration item record for each service asset. This record will contain all operating systems, required applications, optional applications, software updates, security settings, configuration settings, and/or options for the service asset sufficient in detail that allows a low-level technician to deploy a replacement service asset into the N-NC environment and be fully functional.

3.7.5.6.8 Maintain definitive network and logical diagrams per service and overall in a single location and linked to the CMDB. Produce specific diagrams on demand as requested by the Government and Service Owner within request fulfillment timelines.

3.7.5.6.9 Develop a Lifecycle Technical Refresh Plan for IT Service Assets supporting Services in the Service Catalog. Support future budget analysis and recommendations on service asset upgrades and replacement. Implement Government-approved annual technology refresh decisions.

3.7.5.6.10 Provide technical support to maintain existing or new architecture products (DoD Architecture Framework (DoDAF) Standard Views for NORAD and USNORTHCOM mission sets and critical processes. Shall maintain detailed network topology diagrams for each service in the service catalog using the DODAF Architecture Diagrams, Service Systems Matrix, Service Functionality Description, Service Measures Matrix, Service Evolution Description, Service & Technology & Skills Forecast.

3.7.5.7 Outputs

See Appendix E Output Specifications

1. Monthly Service Asset and Configuration Management Report **[CDRL A003]**
2. Monthly Configuration Management Database (CMDB) Report **[CDRL A005]**
3. Monthly Hardware And Software Asset Report **[CDRL A005]**
4. Monthly Software License Utilization Report **[CDRL A005]**
5. Semi-Annual Microsoft True-Up Report **[CDRL A011]**
6. Monthly Equipment Control Officer Report **[CDRL A005]**
7. Annual Lifecycle Technical Refresh Plan **[CDRL A013]**
8. Approved Software Catalog

3.7.5.8 Operational Metrics

A. Total Number Of CIs In CMDB
B. Number Of CI Errors (Omission Or Inaccuracies) Discovered
C. Number Of Incidents Related To Inaccurate CI Information

D. Number Of Change Failures Related To Inaccurate CI Information
E. Number Of Services Operating With Incomplete CI Information
F. Number Of Services In Service Catalog
G. Number Of CIs Without Assigned Ownership
H. Total Changes Implemented
I. Total Number Of Incidents
J. Total Number of Service Assets Received During Reporting Period
K. Total Number of Service Assets Documented in AIMs During Reporting Period
L. Total Number of Service Assets Scheduled for Transfer to DRMO
M. Total Number of Service Assets Transferred to DRMO
N. Total Number of Service Assets Scheduled for Deployment
O. Total Number of Service Assets Deployed
P. Total Number of Service Assets Scheduled for Return to ECO
Q. Total Number of Service Assets Returned to ECO
R. Total Number of Non-Compliant EC Accounts (Annual EC Training, Appointment Letter, and Inventory)
S. Total Number of Non-Compliant EC Accounts Frozen
T. Total Number of Frozen EC Accounts Without Corresponding Report of Survey Initiation Request
U. Total Number of Service Asset Types
V. Total Number of Service Asset Types Without Documented Sanitization Procedures
W. Number of Services with Complete Service Diagrams

3.7.5.9 Key Performance Indicators

3.7.5.9.1 CMDB Accuracy Ratio [Metric: 1-(B/A)]

- *Superior Service Threshold:* 85%
- *Service Warning:* 75%

3.7.5.9.2 Number Of Incidents Related To Inaccurate CI Information [Metric: C/I]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.7.5.9.3 Inaccurate Configuration Item Data Change Failure Rate [Metric: D/H]

- *Superior Service Threshold:* 5%
- *Service Warning:* 10%

3.7.5.9.4 CMDB Completeness Ratio [Metric: 1-(E/F)]

- *Superior Service Threshold: 95%*
- *Service Warning: 90%*

3.7.5.9.5 Configuration Item Ownership Rate [Metric: 1-(G/A)]

Internal

- *Superior Service Threshold (Internal) : 95%*
- *Service Warning (Internal): 85%*

External

- *Superior Service Threshold (External): 85%*
- *Service Warning (External): 75%*

3.7.5.9.6 Service Asset Accountability Index [Metric: K/J]

- *Superior Service Threshold: 98%*
- *Service Warning: 85%*

3.7.5.9.7 Service Asset Retirement Rate [Metric: M/L]

- *Superior Service Threshold: 90%*
- *Service Warning: 70%*

3.7.5.9.8 Service Asset Deployment Rate [Metric: O/N]

- *Superior Service Threshold: 90%*
- *Service Warning: 70%*

3.7.5.9.9 Service Asset Recovery Rate [Metric: Q/P]

- *Superior Service Threshold: 90%*
- *Service Warning: 70%*

3.7.5.9.10 EC Account Compliance Enforcement Index [Metric: S/R]

- *Superior Service Threshold: 95%*
- *Service Warning: 85%*

3.7.5.9.11 Non-Compliant EC Account Forced Reconciliation Rate [Metric: 1-(T/S)]

- *Superior Service Threshold: 90%*
- *Service Warning: 70%*

3.7.5.9.12 Sanitization Procedure Coverage Rate [Metric: 1-(V/U)]

- *Superior Service Threshold: 98%*
- *Service Warning: 85%*

3.7.5.9.13 Service Diagram Coverage Rate [Metric: W/F]

- *Superior Service Threshold: 95%*
- *Service Warning: 85%*

3.7.5.10 Critical Success Factors

- Maintain a Viable and Accurate IT Environment [KPI: 1, 3, 4, 5, 6, 13]
- Maintain Quality IT Services [KPI: 2, 3]
- Deliver Accurate and Timely IT Services [KPI: 6, 7, 8, 9]
- Provide Effective and Efficient IT Service Management [KPI: 5, 10, 11, 12]

3.7.6 **Sub-Task 4: Release and Deployment Management**

3.7.6.5 Overview

Release and Deployment Management aims to build, test, and deliver the capability to provide the services specified by service design and that will accomplish the stakeholder’s requirements and deliver the intended objectives.

The goal of Release and Deployment Management is the deployment of releases into the NORAD and USNORTHCOM production environment and to establish effective use of the service in order to deliver value to the customer. It allows efficient transition of the service into operations.

3.7.6.6 Requirements

The Contractor Shall:

3.7.6.6.1 Provide, integrate, and manage Release and Deployment Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.6.6.2 Develop and document Release and Deployment Package(s) for all approved Service Design Packages. Release and Deployment Packages will be coordinated with and presented to the Government for engineering board review and acceptance. The Contractor shall review and participate in engineering and/or release review boards for Third-Party produced Release and Deployment Packages.

3.7.6.6.3 Obtain Government CAB approval to all non-emergency Request for Change(s) to a minimum of 10 business days prior to start of change implementation.

3.7.6.6.4 Provide Evaluation Reports for Third-Party Release and Deployment Packages within 10 (ten) business days of receipt from the Government. Exceptions to meeting the specified time must be requested to the Government within the 3 (three) business days with a justification and an expected delivery date for report completion.

3.7.6.7 Outputs

See Appendix E Output Specifications

1. Monthly Release And Deployment Report **[CDRL A003]**
2. Release And Deployment Package(s)

3.7.6.8 Operational Metrics

A. Number of Scheduled Release and Deployment Packages
B. Total Releases Implemented IAW release date
C. Number Of Failed Releases
D. Number Of Scheduled Release and Deployment Packages Approved

3.7.6.9 Key Performance Indicators

3.7.6.9.1 Release Success Rate [Metric: 1-(C/B)]

- *Superior Service Threshold:* 90%
- *Service Warning:* 80%

3.7.6.9.2 Release Schedule Rate [Metric: D/A]

- *Superior Service Threshold:* 95%
- *Service Warning:* 80%

3.7.6.10 Critical Success Factors

- Implement Quality IT Services [KPI: 1]
- Provide Effective and Efficient IT Service Management [KPI: 1, 2]

3.7.7 Sub-Task 5: Service Validation and Testing

3.7.7.5 Overview

Service Validation and Testing is a process that contributes to quality assurance and ensures that the service delivered matches its design specification and will deliver a new or changed service that is fit for purpose and fit for use.

The goal of Service Validation and Testing is to ensure that a service adds value to and meets NORAD and USNORTHCOM's operational and mission needs.

A NORAD and USNORTHCOM Test and Integration Laboratory (TIL) currently exists and is in-use. Details on TIL assets will be provided in the Technical Library.

3.7.7.6 Requirements

The Contractor Shall:

3.7.7.6.1 Provide, integrate, and manage Service Validation and Testing to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.7.6.2 Operate and maintain a test and integration facility to test and validate hardware and software interoperability, enhancements, and new technology against the NORAD and USNORTHCOM IT enterprise baseline. Test environment will replicate the NORAD and USNORTHCOM operational network and support IT service technology integration, testing, training and development of capabilities prior to release and deployment on operational networks.

3.7.7.7 Outputs

See Appendix E Output Specifications

1. Monthly Service Validation and Test Report **[CDRL A003]**
2. Configuration Baselines Of The Test Environment
3. Validation and Test Plan(s)
4. Validation and Test Results Report(s)
5. Service Release Report(s)
6. Artifacts For Certification and Accreditation of Release Package
7. Service Acceptance Criteria

3.7.7.8 Operational Metrics

A. Total Number Of Service Acceptance Tests Plans Completed (per Deployment for New or Changed Service)
B. Number of Service Acceptance Test Results Reported (per Deployment for New or Changed Service)
C. Total Number of Service Operational Test Plans Completed (per SDP)
D. Number of Service Operational Test Results Reported (per SDP)
E. Total Number of Service Release Test Plans Completed (per RDP)
F. Number of Service Release Test Results Reported (per RDP)
G. Total Number of Component and Build Test Plans Completed
H. Number of Component and Build Results Reported
I. Total Number Of Release Packages Tests Scheduled Per Month
J. Total Number Of Incidents
K. Number of Incidents Caused by New or Changed Services

3.7.7.9 Key Performance Indicators

3.7.7.9.1 Service Acceptance Test Plan Coverage [Metric: B/A]

- *Superior Service Threshold:* 100%
- *Service Warning:* 90%

3.7.7.9.2 Service Operational Test Plan Coverage [Metric: D/C]

- *Superior Service Threshold:* 95%
- *Service Warning:* 85%

3.7.7.9.3 Service Release Test Plan Coverage [Metric: F/E]

- *Superior Service Threshold:* 95%
- *Service Warning:* 85%

3.7.7.9.4 Service Component and Build Test Plan Coverage [Metric: H/G]

- *Superior Service Threshold:* 90%
- *Service Warning:* 80%

3.7.7.9.5 Release Incident Impact Rate [Metric: K/J]

- *Superior Service Threshold:* 3%
- *Service Warning:* 5%

3.7.7.9.6 Test Timeliness Calculation [Metric: ((F+H)/I)]

- *Superior Service Threshold:* 90%
- *Service Warning:* 80%

3.7.7.10 Critical Success Factors

- Implement Quality IT Services [KPIs: 1, 2, 3, 4]
- Deliver Accurate and Timely IT Services [KPIs: 1, 2, 6]
- Optimize Overall Mission Risks [KPIs: 5]

3.7.8 **Sub-Task 6: IT Knowledge Management**

3.7.8.5 Overview

IT Knowledge Management is responsible for gathering, analyzing, storing, training, and sharing knowledge and information within an organization regarding ITSM services and best practices. This process ensures the right information is delivered to the right place or person at the right time in order to enable informed decisions among the IT services lifecycle.

The goal of knowledge management is to improve the quality of the Government's ITSM Services decision making process by ensuring that reliable and secure information is available during the service lifecycle.

3.7.8.6 Requirements

The Contractor Shall:

3.7.8.6.1 Provide, integrate, and manage IT Knowledge Management to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.8.6.2 Responsible for creating, maintaining, and updating a portal-based repository on the N-NC unclassified portal of all Contractor produced outputs, metrics, and documentation as part of the Contractor's knowledge management system.

3.7.8.6.3 Develop and conduct user training and awareness plans for new or significantly modified network services. Coordinate and provide an IT Service Management overview brief for the monthly NORAD and USNORTHCOM newcomers brief.

3.7.8.7 Outputs

See Appendix E Output Specifications

1. Monthly Knowledge Management Report **[CDRL A003]**
2. IT Knowledge Management Plan(s)
3. Orientation And Training Package(s)

3.7.8.8 Operational Metrics

A. Number Of N2ITSM Contractor Supported Services In Service Catalog
B. Number Of Services Without Complete Training Package (e.g. User, Executive, Technical)
C. Number Of Training Sessions Scheduled
D. Number Of Training Sessions Conducted
E. Total Number Of Service Assets By Type
F. Number Of Service Assets Without Documented TTPs (e.g. Install, Maintenance, Recovery Instructions)
G. Total Number Of Incidents By Type
H. Number Of Incident Types With Inaccurate, Incomplete, Or Missing Documented Workarounds

3.7.8.9 Key Performance Indicators

3.7.8.9.1 IT Service Training Package Coverage Rate [Metric: 1-(B/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.7.8.9.2 IT Service Training Execution Rate [Metric: D/C]

- *Superior Service Threshold:* 95%
- *Service Warning:* 90%

3.7.8.9.3 Service Asset Documented Procedure Rate [Metric: 1-(F/E)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 90%

3.7.8.9.4 Incident Workaround Coverage Rate [Metric: 1-(H/G)]

- *Superior Service Threshold:* 90%
- *Service Warning:* 80%

3.7.8.10 Critical Success Factors

- Optimize User/Customer IT Awareness [KPI: 1, 2]
- Improve Mission /Business Productivity with IT Services [KPI: 1, 2, 3]
- Effective Communications with Users [KPI: 3, 4]

3.7.9 **(Optional Task) Sub-Task 7: Change Evaluation**

3.7.9.5 Overview

Change Evaluation is the process to provide a consistent and standardized means of determining the performance of a service change in the context of existing and proposed services and IT service assets.

The goal of the ITIL evaluation process is to determine the performance of a service change based on the predicted (intended) performance.

3.7.9.1.1 Requirements

The Contractor Shall:

3.7.9.5.1 Provide, integrate, and manage Change Evaluation to meet Government specified outputs, Operational Metrics, Key Performance Indicators, and Critical Success Factors identified below. The Government will review and validate reports and documents provided by the Contractor and provide feedback.

3.7.9.5.2 Develop and document Evaluation Plan(s) and Report(s) that ensures that:

- Evaluation of service changes prior to implementation
- User acceptance testing to include customer involvement
- How unintended effects and risks of a change and its consequences must be identified
- How a change will be evaluated fairly, consistently, openly and objectively
- Evaluation of each new or significantly changed service approved by the Government which include, but are not necessarily limited to evaluating the predicted performance, evaluating the actual performance, service acceptance criteria, and test report.

3.7.9.5.3 Provide Evaluation Reports for Third-Party Service Design Packages and Release and Deployment Packages within 10 (ten) business days of receipt from the Government. Exceptions to meeting the specified time must be requested to the Government within the 3 (three) business days with a justification and an expected delivery date for report completion.

3.7.9.6 Outputs

See Appendix E Output Specifications

1. Monthly Evaluation Management Report **[CDRL A003]**
2. Evaluation Report(s)

3.7.9.7 Operational Metrics

A. Total Number Of MAJOR Changes Completed; Monthly
B. Number Of MAJOR Changes Completed Without Post-Implementation Review; Monthly
C. Number Of MAJOR Changes Completed Without Release Deployment Package (RDP) Review; Monthly
D. Number Of MAJOR Changes Completed Without Service Design Package (SDP) Review; Monthly
E. Number Of MAJOR Changes Completed Without Service Package (SP) Review; Monthly

3.7.9.8 Key Performance Indicators

3.7.9.8.1 MAJOR Change Evaluation After Deployment Rate [Metric: 1-(B/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.7.9.8.2 MAJOR Change Evaluation Prior to Deployment [Metric: 1-(C/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.7.9.8.3 MAJOR Change Evaluation Prior to Build [Metric: 1-(D/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.7.9.8.4 MAJOR Change Evaluation Prior to Planning [Metric: 1-(E/A)]

- *Superior Service Threshold:* 98%
- *Service Warning:* 95%

3.7.9.9 Critical Success Factors

- Optimize Overall Mission Risks [KPI: 1, 2, 3, 4]
- Improve the Quality of IT Service Management Decisions [KPI: 1, 2, 3]
- Implement Quality IT Services [KPI: 1, 2, 3]

3.8 Task 6: Continuous Service Improvement

3.8.1 Overview

Service Improvement is the continuous review and analysis, at a minimum, of the functions, processes, outputs, and IT services specified in this PWS to make recommendations to the Government on improvement opportunities.

The goal is to improve IT service quality and the efficiency and effectiveness of all enabling IT Service Management functions and processes.

3.8.2 Requirements

The Contractor shall:

3.8.2.5 Provide recommendations to the Government for Service Improvements based on information and data that was measured, collected/gathered, processed and analyzed. Provide courses of action for all improvement recommendations for Government consideration and decision-making.

3.8.2.6 Review and analyze service level targets, process metrics and performance indicators, output specifications, and any other Contractor items of interest quarterly and provide the Government recommendations for improvements.

3.8.3 Outputs

See Appendix E Output Specifications

1. Quarterly Process and Service Improvement Report **[CDRL A006]**

3.9 Task 7: Projects

3.9.1 Overview

This section outlines the Government's requirement for work which is not specifically identified in the PWS, but which is still within the general scope of this contract. The Government anticipates using separate PWS's, to be determined by the Contracting Officer on a case-by-case basis. Firm Fixed Price contracts will be negotiated by the Contracting Officer and work shall commence when the contract modification is awarded.

The Government retains the authority to award a new or changed service in accordance with the Contractor provided Service Package. The Contractor is required to be efficient in Service Package development and will be held responsible for the Service Package specified cost, schedule, and performance. The Government retains the right to openly compete the Contractor provided Service Package and award the project to a Third Party, if but not limited to, the Contractor provided Service Package being incomplete, inaccurate, and/or over estimated total cost of ownership.

3.9.2 *Requirements*

The Contractor shall:

3.9.2.5 Projects at Contract Start

3.9.2.1.1 Be prepared to support Service Transition activities for projects that will be in the service pipeline at contract start. The Contractor shall have the capabilities to provide project integration, coordination, and technical management expertise required to support ongoing projects. In particular, those projects that are core service migrations to the infrastructure (e.g. MS Windows 7 upgrade). The Service Pipeline for projects that the Government anticipates will be ongoing at contract start are in the Technical Library.

3.9.2.6 Projects Awarded to the N2ITSM Contractor

3.9.2.6.1 Provide the Government implementation and sustainment costs for the new or changed service as part of the Service Package. The Government will execute projects as separate project CLINs. If the Government accepts the project proposal, the sustainment cost will be added to the annual contract value as a contract modification.

3.9.2.6.2 Upon project award/contract modification the Contractor is responsible for Service Design, Service Transition, Early Life Support , and Service Operations tasks as required in this PWS

3.9.2.7 Projects Implemented by Third-Party Contractor(s)

3.9.2.7.1 Facilitate Design Coordination and Transition Planning and Support tasks to ensure the third-party new or changed service(s) are transitioned to Service Operations. The Contractor is responsible for integration of Service Strategy Support, Service Design, Service Transition, and Service Operations tasks as required in this PWS to ensure complete integration into the N-NC Enterprise Service Portfolio and Catalog.

Estimate 5 (five) Third-Party projects per quarter.

3.9.2.7.2 Provide integration and coordination of the Third-Party's Service Design Package, Release and Deployment Package, Requests for Changes, Early Life Support Plan, and Project Plan.

3.9.2.7.3 Perform project integration to ensure that Third-Party project deliverables and project activities are coordinated and executed within the Contractor's ITSM organization.

3.9.2.7.4 Provide Government Change Advisory Board recommendations to Third-Party change requests and service life-cycle packages and plans. Identify constraints and limitations to tasks assigned to the Contractor as identified in the Third-Party's project plan.

3.9.2.7.5 Provide the Government annual Service Operations sustainment costs for Third-Party provided new or changed services. If the Government accepts, the Service Operations Firm Fixed Price contract value will be modified to include the new or changed service sustainment cost.

3.9.3 *Outputs*

See Appendix E Output Specifications

1. Project Integration Criteria

4 Deliverables and Outputs.

Contractor shall deliver all outputs in accordance with Contract Data Requirements List DD Form 1423 and Table 4-1. Quarterly reports are due in March, June, September and December. Semi-Annual reports are due in April and October. Annual reports are due In April, unless otherwise indicated in the Output Specification. These are delivered in accordance with the normal reporting delivery schedule and for the previous months.

Table 4-1. *Timelines for Deliverables and Outputs*

Number	CDRL	Subtask	Document Number	Description	Frequency
1	A001	3.3.1 Process Models	3.3.1-1	Implementation Plan	Once, 30 days after Contract Award
2	A002	3.3.1 Process Models	3.3.1-2	Process Models	Once, 30 days after Contract Start
3	A003	3.4.1 Service Desk	3.4.1.1-1	Monthly Service Desk Call Report	Monthly
4	A003	3.4.2 Incident Mgmt	3.4.2.2-1	Monthly Incident Management Report	Monthly
5		3.4.2 Incident Mgmt	3.4.2.2-2	Monthly SLA/OLA Breach Report	Monthly
6		3.4.2 Incident Mgmt	3.4.2.2-3	Major Incident Report	As Needed
7	A003	3.4.3 Request Fulfillment	3.4.3.3-1	Monthly Request Fulfillment Report	Monthly
8	A003	3.4.4. Access Mgmt	3.4.4.4-1	Monthly Access Management Report	Monthly
9		3.4.4. Access Mgmt	3.4.4.4-2	Unauthorized Access and Rights Escalation Report	As Needed - Within 6 hours of incident
10	A006	3.4.4. Access Mgmt	3.4.4.4-3	Quarterly Access Management Report	Quarterly
11	A003	3.4.6 Problem Mgmt	3.4.6.6-1	Monthly Problem Management Report	Monthly
12	A004	3.4.6 Problem Mgmt	3.4.6.6-2	Monthly Known Error Database (KEDB)	Monthly
13		3.4.6 Problem Mgmt	3.4.6.6-3	Root Cause Analysis Report(s)	As Needed
14		3.4.9 Network Operations Center Spt	3.4.9-1	Daily Operations Brief Input	Daily
15	A003	3.4.10 Monthly Event Mgmt	3.4.10.9-1	Monthly Event Management Report	Monthly
16		3.4.10 Event Management	3.4.10.9-2	Event Monitoring Plan	Semi-Annual
17	A003	3.5.2 Service Portfolio Mgmt	3.5.2.1-1	Monthly Service Portfolio Management Report	Monthly
18		3.5.2 Service Portfolio Mgmt (Option)	3.5.2.1-2	(Optional Task) Mission Case(s)	As Needed
19		3.5.2 Service Portfolio Mgmt	3.5.2.1-3	Service Package(s)	As Needed
20		3.5.2 Service Portfolio Mgmt	3.5.2.1-4	Non-Standard Request Analysis Report	As Required
21		3.5.2 Service Portfolio Mgmt	3.5.2.1-5	Investment Analysis Report	As Required
22	A003	3.5.3 ITSM Financial Mgmt	3.5.3.2-1	Monthly ITSM Financial Management Report	Monthly
23	A010	3.5.3 ITSM Financial Mgmt	3.5.3.2-2	Semi-Annual ITSM Budget Forecast Report	Semi-Annual
24	A010	3.5.3 ITSM Financial Mgmt	3.5.3.2-3	Semi-Annual ITSM TCO Report	Semi-Annual
25	A003	3.5.4 Demand Mgmt (Option)	3.5.4.3-1	Monthly Demand Management Report	Monthly
26		3.5.4 Demand Mgmt (Option)	3.5.4.3-2	Patterns of Business Activity	Annual
27		3.5.4 Demand Mgmt (Option)	3.5.4.3-3	User Profiles	Annual
28	A007	3.6.5 IT Enterprise Architecture (Option)	3.5.5.4-1	Quarterly Architecture Products and Updates	Quarterly
29		3.6.2 Design Coordination	3.6.2.1-1	Service Design Package(s)	As Needed
30	A003	3.6.3 Service Level Mgmt	3.6.3.2-1	Monthly Service Level Management Report	Monthly
31		3.6.3 Service Level Mgmt	3.6.3.2-2	Service Level Agreement(s)	Annual
32		3.6.3 Service Level Mgmt	3.6.3.2-3	Operational Level Agreement(s)	Annual
33	A003	3.6.4 Service Catalog Mgmt	3.6.4.3-1	Monthly Service Catalog Report	Monthly
34		3.6.4 Service Catalog Mgmt	3.6.4.3-2	Service Catalog	As Needed
35		3.6.4 Service Catalog Mgmt	3.6.4.3-3	Core Service Package(s)	As Needed, 90 days after contract start
36		3.6.4 Service Catalog Mgmt	3.6.4.3-4	Service Level Package(s)	As Needed, 90 days after contract start
37	A003	3.6.5 Supplier Mgmt	3.6.5.4-1	Monthly Supplier Management Report	Monthly
38		3.6.5 Supplier Mgmt	3.6.5.4-2	Procurement Package(s)	As Required
39		3.6.5 Supplier Mgmt	3.6.5.4-3	Underpinning Contract Recommendation(s)	Monthly
40	A003	3.6.6 Information Security Mgmt	3.6.6.5-1	Monthly Information Security Management Report	Monthly
41		3.6.6 Information Security Mgmt	3.6.6.5-2	Plan of Actions and Milestones	As Needed
42		3.6.6 Information Security Mgmt	3.6.6.5-3	Certification and Accreditation Package(s)	As Needed
43		3.6.6 Information Security Mgmt	3.6.6.5-4	Circuit Request(s)	As Needed
44		3.6.6 Information Security Mgmt	3.6.6.5-5	Cross Domain Request(s)	As Needed
45		3.6.6 Information Security Mgmt	3.6.6.5-6	Techical Review Sheet(s)	As Needed
46	A006	3.6.6 Information Security Mgmt	3.6.6.5-7	Quarterly Information Security Management Report	Quarterly
47	A003	3.6.7 Availability Mgmt	3.6.7.6-1	Monthly Availability Management Report	Monthly
48		3.6.7 Availability Mgmt	3.6.7.6-2	Availability Management Plan(s)	Annual
49	A003	3.6.8 Capacity Mgmt	3.6.8.7-1	Monthly Capacity Management Report	Monthly
50		3.6.8 Capacity Mgmt	3.6.8.7-2	Capacity Management Plan(s)	Annual
51	A008	3.6.8 Capacity Mgmt	3.6.8.7-3	Quarterly IT Service Utilization Report	Quarterly
52	A003	3.6.9 IT Service Continuity Mgmt	3.6.9.8-1	Monthly IT Service Continuity Report	Monthly
53	A012	3.6.9 IT Service Continuity Mgmt	3.6.9.8-2	IT Service Mission Impact Analysis	Annually, 60 days after Contract Start and Annually thereafter
54		3.6.9 IT Service Continuity Mgmt	3.6.9.8-3	IT Service Continuity Plan(s)	Annual
55	A009	3.6.9 IT Service Continuity Mgmt	3.6.9.8-4	Quarterly IT Service Continuity Test & Audit Schedule	Quarterly
56	A009	3.6.9 IT Service Continuity Mgmt	3.6.9.8-5	Quarterly IT Service Continuity Test & Audit Report	Quarterly

Table 4-1. Timelines for Deliverables and Outputs (Continued)

Number	CDRL	Subtask		Description	Frequency
57		3.7.2 Transition Planning and Support	3.7.2.1-1	Project Transition Brief Input	Weekly
58		3.7.2 Transition Planning and Support	3.7.2.1-2	Early Life Support Package(s)	As Required
59	A003	3.7.3 Change Mgmt	3.7.3.2-1	Monthly Change Management Report	Monthly
60		3.7.3 Change Mgmt	3.7.3.2-2	Forward Schedule of Changes	Daily
61		3.7.3 Change Mgmt	3.7.3.2-3	Request for Change	As Needed
62		3.7.3 Change Mgmt	3.7.3.2-4	Standard Change Model	As Needed
63	A003	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-1	Monthly Service Asset and Configuration Management	Monthly
64	A005	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-2	Monthly Configuration Management Database Report	Monthly
65	A005	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-3	Monthly Hardware and Software Service Asset Report	Monthly
66	A005	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-4	Monthly Software License Utilization Report	Monthly
67	A011	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-5	Microsoft True-Up Report	Semi-Annual
68	A005	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-6	Monthly Equipment Control Officer Report	Monthly
69	A013	3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-7	Annual Lifecycle Technical Refresh Plan	Annually, 120 days after Contract Start and Annually thereafter
70		3.7.4 Service Asset and Configuration Mgmt	3.7.4.3-8	Approved Software Catalog	As Needed
71	A003	3.7.5 Release and Deployment Mgmt	3.7.5.4-1	Monthly Release and Deployment Report	Monthly
72		3.7.5 Release and Deployment Mgmt	3.7.5.4-2	Release and Deployment Package(s)	As Needed
73	A003	3.7.6 Service Validation and Test	3.7.6.5-1	Monthly Service Validation and Test Report	Monthly
74	A006	3.7.6 Service Validation and Test	3.7.6.5-2	Configuration Baseline of the Test Environment	Quarterly
75		3.7.6 Service Validation and Test	3.7.6.5-3	Validation and Test Plan(s)	As Needed
76		3.7.6 Service Validation and Test	3.7.6.5-4	Validation and Test Results Report(s)	As Needed
77		3.7.6 Service Validation and Test	3.7.6.5-5	Artifacts for Certification & Accreditation of Release	As Needed
78		3.7.6 Service Validation and Test	3.7.6.5-6	Service Acceptance Criteria	As Needed
79	A003	3.7.7 IT Knowledge Mgmt	3.7.7.6-1	Monthly IT Knowledge Management Report	Monthly
80		3.7.7 IT Knowledge Mgmt	3.7.7.6-2	IT Knowledge Management Plan(s)	Annual
81		3.7.7 IT Knowledge Mgmt	3.7.7.6-3	Orientation and Training Package(s)	As Needed
82	A003	3.7.8 Change Evaluation Mgmt (Option)	3.7.8.7-1	Monthly Change Evaluation Management Report	Monthly
83		3.7.8 Change Evaluation Mgmt (Option)	3.7.8.7-2	Change Evaluation Report(s)	As Needed
84	A006	3.8 Continual Service Improvement	3.8.6-1	Quarterly Process and Service Improvement Report	Quarterly
85		3.9 Projects	3.9.7-1	Project Integration Criteria	As Needed
86	A013	8.27 Direct Labor Hour Report	8.27	Report for Contractor's Direct Labor Hours	Annually

5 Deliverable Schedule

All deliverables and outputs will be provided to the Government as per the frequency and times specified in Para 4 in this PWS. The Contractor shall accomplish the milestones shown in Table 4-1.

6 Government Furnished Items and Services.

The Government will provide information on Government-owned and maintained facilities for all full time, direct support. Both Government and Contractor personnel shall jointly occupy the facilities. Office furnishings in appropriate quantities and quality, as determined by the Government, to include desks, chairs, tables, bookcases, safes, and file cabinets, shall be provided for those tasks required to be performed in the Government facilities.

The Government will provide the following computing equipment for no more than 50 seats for Contractor personnel operating at the NORAD and USNORTHCOM HQs:

- Unclassified Workstation with Connectivity to the NORAD and USNORTHCOM NIPRNET
- Classified Workstation(s) with Connectivity to the NORAD and USNORTHCOM SIPRNET and RELCAN
- Desk Phone
- Access to Printers, Faxes, Digital Senders on all Networks

The Contractor shall be responsible for providing all other equipment and property required to execute the provisions of this PWS.

Contractor will be provided access to Government-owned and maintained facilities during normal business hours. NORAD and USNORTHCOM shall provide access, badges, and escorts to the Base and Facilities as required.

6.5.1 Government-Furnished Property Management

The Government will provide an Information Technology Equipment (ITE) Warehouse for the use of government furnished equipment receiving and storage. The Contractor shall account for all Government property using a Contractor-developed property control system in compliance with Federal Acquisition Regulation (FAR) Subpart 45. The Contractor shall account for expendables and all other items previously unaccounted for into an accountability system that satisfies the requirements of the FAR.

6.5.2 Use and Disposition of Government-Furnished Property, Equipment, and Intellectual Property

All official records, files, documents and working papers provided by the Government or generated by the Government in support of the requirements in this PWS are official Government records and shall be added to the Technical Library. The Contractor shall not retain any equipment purchased under this contract or Government provided Intellectual Property for any reason other than the performance of the requirements in this PWS. Contractor shall adhere to Air Force (AFMAN 33-282) procedures for modification and disposition of classified IT hardware or portable media.

7 Contractor Furnished Items and Services.

The Contractor shall provide all necessary Items and Services to perform this PWS unless otherwise provided by the Government.

8 Other Information and Special Conditions

8.5 Hours of Work.

Contractor will, at a minimum:

- Provide telephone service response 24/7/365.
- Provide 24/7/365 support for all services in accordance with ITSM priorities established in this PWS.
- Provide support to exercises and contingencies 24/7.

8.6 Place of Performance.

8.6.1 Locations

8.6.1.1 Primary On-Site

The primary location for contract performance is NORAD and USNORTHCOM Headquarters, located in Building 2, Peterson Air Force Base (AFB), Cheyenne Mountain Air Force Station, and Colorado Springs, Colorado area. The Contractor is required to support all locations served by the NORAD and USNORTHCOM IT Enterprise identified in Para 2.1 and Table 2-1 of this PWS. On-site support requires manning at that location to meet service levels. On-site support for the Peterson AFB, Cheyenne Mountain Air Force Station, and Colorado Springs, CO areas are considered local travel and will not be reimbursed.

8.6.1.2 Contractor Off-Site

The Contractor is allowed and expected to work outside of NORAD and USNORTHCOM HQs to the maximum extent possible. The allotment of Government-provided Contractor on-site workspace is limited to 50 seats with 24/7 access. Government, upon approval, will provide at the Contractor’s off-site facility NIPR and SIPR workstations and printers. The Contractor will be responsible for transport and infrastructure to N-NC Headquarters, Bldg. 2 for NIPR and SIPR access.

Number of Seats Provided	Room	Location/Facility
12	B038	Bldg 2 Office Space
10	B030	Bldg 2 VTC Technical Space
3	B042	Bldg 2 Computer Support Space
5	B058	Bldg 2 Network Management Technical Space
5	B010	Bldg 2 Server Farm Technical Space
3	N2C2	Bldg 2 N-NC Command Center (24/7 TS/SCI)
4	NOC	Bldg 2 Network Operations Center (24/7 TS/SCI)
9	123	Bldg 2 Service Desk

Table 8-1. *Contractor Seating Allotment*

8.7 Travel.

Travel may be required in support of this contract anywhere in the NORAD AOO and the NORAD and USNORTHCOM AOR. The travel CLIN on this contract is for Government-directed travel, not local travel. Travel within a 100-mile radius of Peterson AFB is considered “local travel.” Any location within the local travel area at which the Contractor may be required to perform duties required in the PWS shall be an alternate duty location. When travel outside the local Peterson complex is required, the Contractor shall obtain written approval from the SQAE or FCO a minimum of five days prior to travel commencing. Travel requests shall include relevant PWS paragraph reference, approximate travel dates, expected duration, origin and destination, purpose, estimated costs and number/names of personnel traveling. Travel reimbursement shall be IAW Federal Acquisition Regulation (FAR) 31.205-46, on a cost-reimbursable basis.

8.8 Applicable Directives.

All applicable directives to meet the requirements and to comply in performance of this PWS are included but not limited to those referenced in the Technical Library.

8.9 Disaster Preparedness.

8.9.1 Contingencies and Exercises

The Contractor shall support two major exercises (e.g. Vigilant Shied and Ardent Sentry) and between 2-6 minor exercises per year. Major exercises may last 7-12 days, minor exercises may last 2-3 days each. The Contractor shall set up 2-4 temporary battle cells consisting of up to 100 positions total with workstations, printers, and other peripheral devices. These positions will be priority 1A for the duration of the exercise. The Contractor shall provide an exercise contact and recall rosters for all major exercises and contingencies, the Contractor is expected to have adequate Service Desk, IT Operations, Technical Management, and Application Management staffing to support major exercises and contingencies; shifting adjustments to support 24/7 operations is required.

The Contractor is responsible supporting all tasks in this PWS during contingency operations. If a contingency requires additional services then the Government may consider executing the Contingency CLIN to acquire those services. The Contractor shall be prepared to execute Disaster Recovery and Continuity of Operations during all exercises and contingencies.

8.9.2 Workforce Contingency Planning

The Contractor shall develop a contingency plan for continued contract support in the event of a declared crisis, catastrophic and non-catastrophic events and work stoppages. The plan shall contain the following information at a minimum: contingency actions, emergency work requests, natural disasters, labor strike/personnel walk-off, contingency mobilization and mobilization recall commitments. Provide a copy of the contingency plan at contract start and updates as changes occur.

8.10 Technical Meetings, Conferences, and Information Requests

The Contractor shall participate in and provide technical support and/or documentation for Government meetings as required. The level of support required varies based on the meeting being supported and includes, but is not limited to, administration, organization, subject matter expert (SME), and meeting minutes, or any combination thereof. The Contractor is required to provide coordination, feedback, comments, or recommendations on Contractor produced outputs and Third-Party produced documents, such as but not limited to,

- Service Design Packages
- Release and Deployment Packages
- Service Validation and Test Plans and Results
- Early Life Support Plans
- Request for Changes

The Contractor shall provide an initial response within 2 hours to information requests from Contracting Officer's Representative. Information request(s) may be generated by leadership, management, and/or Government oversight to address current and/or future IT Service Management issues, concerns, and topics.

8.11 Program Management Reviews (PMRs)

The Contractor shall present data to facilitate a joint review of Contractor’s performance based on process and function Key Performance Indicators and Critical Success Factors. The Contractor shall identify performance deficiencies and provide corrective actions and recommendations. PMRs shall be conducted on a monthly basis, but may be reduced to a quarterly basis at the discretion of the Contracting Officer and Customer Program Manager.

8.12 Referenced Publications

The Contractor shall comply with the requirements cited in referenced publications, unless waivers are granted by the appropriate Government official (e.g., Designated Approving Authority (DAA), FCO). The list of publications is located in Appendix A.

8.12.1 Changes

The Contractor shall notify the Contracting Officer (CO) of any changes in publications listed in Appendix A within 30 days of receipt of revisions, changes, supplements and notifications of rescission which may impact contract cost. The Contractor shall immediately implement no cost changes, revisions, and supplements. Before implementing any change that will result in an increase in contract price, the Contractor shall submit a price proposal to the CO within 30 calendar days following receipt of the change by the Contractor. The CO and the Contractor will negotiate the change into the contract under the provisions of the contract clause entitled “Changes.” Failure of the Contractor to submit a price proposal within 30 calendar days following receipt of the change, revision and supplement entitles the Government to performance according to such change at no increase in contract price. When revisions, changes and supplements involve safety, classified control or mission degradation, notify the CO by email within 24 hours of receipt of the publication and advise as to whether a cost impact has been created.

8.13 Operational Level Agreement (OLA) and Service Level Agreement (SLA)

The Contractor shall comply with the requirements in approved OLAs and SLAs and maintain current copies in the Technical Library. All existing SLAs/OLAs will be provided in the Technical Library.

8.14 Records Management

8.14.1 Compliance and Approval

Contractor agrees to comply with Federal and N-NC records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format [paper, electronic, etc.] or mode of transmission [e-mail, fax, etc.] or state of completion [draft, final, etc.]. No disposition of documents will be allowed without the prior written consent of the Command Records Manager. The N-NC and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of N-NC or destroyed without regard to the records schedule in CJCSM 5760.01A Vol II.

Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and N-NC guidance for protecting sensitive and proprietary information.

8.14.2 Creation, Dissemination, and Maintain

Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which N-NC shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using N-NC IT equipment and/or N-NC records. Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act. Contractor shall not create or maintain any records containing any N-NC records that are not specifically tied to or authorized by the contract.

8.14.3 Records Ownership

N-NC owns the rights to all data/records produced as part of this contract. N-NC owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit N-NC to use the data.

8.15 Reports

The Contractor shall provide electronic reports to the Government for all Contract Deliverable Requirement Lists (CDRLs). Provide reports as specified in this PWS for processes and functions (e.g., outputs) within the required timeframes. Contractor format is acceptable unless specified otherwise.

8.15.1 Correspondence

The Contractor shall provide correspondence/reports and communications developed by the Contractor and intended for release to individuals other than those involved with the immediate management of the contract (Functional Commander, Contracting Officer, Government Program Manager, Contractor Officer's Representative (COR) must be approved by the SQAE or FCO prior to release.

8.16 Technical Library

The Technical Library allows bidding Contractors access to all applicable documentation in a centralized location and is maintained by the Contractor and available to the Government at all times. The content of the Technical Library includes, but is not necessarily limited to, the following:

1. NORAD and USNORTHCOM Instructions, Policies
2. N-NC Service Catalog and Hardware and Software Asset Lists
3. Operating Instructions (OIs), SLAs, OLAs, MOUs, Underpinning Contracts, etc.
4. Copies of the monthly PMR meeting minutes
5. Output Specifications

The Contractor shall maintain and update all documentation and databases contained within the Technical Library as changes occur and incorporate records/reports generated in performance of PWS requirements and operation/maintenance manuals for newly acquired equipment/software into the library. The Technical Library will be posted and made available to the appropriate Government POCs at all times, and ownership will be transferred to the Government upon contract completion.

8.17 Information and Documentation

All information and documentation generated and maintained under this contract must be made available for Government review upon request.

8.18 Freedom of Information Act (FOIA) and Privacy Act (PA) Requests

The Contractor shall forward FOIA and PA requests received to HQ/N-NC/CS. The Contractor shall safeguard PA and For Official Use Only (FOUO) materials in accordance with applicable policies and regulations.

8.19 Contract Program Manager (CPM)

The Contractor shall identify a CPM who will serve as the primary POC with the Government on matters of contract performance. The Contractor shall provide written notification of the name, work phone number, and alternate phone numbers of the CPM and his or her alternate to the CO not later than the pre-performance conference and within five calendar days of any subsequent changes thereafter. CPM or alternate shall have full authority to act for the Contractor on all matters relating to the day-to-day operation of this contract, and will be, or his or her alternate, have contact availability 365/7/24.

During NORAD and USNORTHCOM normal business hours, the CPM or alternate shall be available within 1 hour to meet at the NORAD and USNORTHCOM complex with Government personnel to discuss PWS requirements and issues/concerns. After NORAD and USNORTHCOM normal business hours (weather permitting), the CPM or alternate shall be on site within 2 hours.

8.20 Contractor Personnel

Contractor personnel shall adhere to established procedures in the event of actual or simulated fires, weather advisories, natural disasters, bomb threats, terrorist activities, enemy attack and other similar emergency conditions posing a real or potential danger to people or property. The Contractor shall follow the NORAD and USNORTHCOM and Peterson AFB Emergency Action Plans.

8.21 Training

The Contractor shall incur all costs for training Contractor personnel to meet the requirements of the PWS. The Government shall incur no Contractor training costs under this PWS except for one-time training for DoD proprietary newly implemented IT service assets for operational or administrative downward directly implementation not common to the commercial industry market. Contractor shall have received all required information assurance training and possess all required information assurance certifications at contract start, and will comply with mandatory NORAD and USNORTHCOM information security awareness and periodic refresher training. The Contractor shall comply with all training requirements in NORAD and USNORTHCOM Instruction, 36-138.

8.22 Safety

The Contractor shall report safety mishaps/incidents involving Contractor personnel to the SQAE or FCO within 24 hours of an incident, and shall assist with mishap investigations that involve Contractor personnel. The Contractor shall comply with all Federal, State, DoD, and N-NC safety regulations, policies, and guidelines.

8.23 Industrial Security

The Contractor shall comply with National Industrial Security Program (NISPOM), information security management and security and law enforcement procedures and plans established for NORAD and USNORTHCOM and Peterson AFB.

8.24 Physical Security

The Contractor shall comply with base Operations and Disaster Preparedness Plans and Instructions for Force Protection Condition procedures, Random Anti-terrorism Measures and local search and identification requirements. The Contractor shall adhere to NORAD and USNORTHCOM security polices and be responsible for safeguarding Government property provided for Contractor use. Secure all equipment, materials and Government facilities at the end of each work day.

8.25 Entry Procedures for Controlled and Restricted Areas

The Contractor shall comply with and enforce entry and internal controls/other physical security requirements for Contractor-controlled areas.

The Contractor shall limit requests for restricted area unescorted entry access to employees whose duties require entry to such area(s) more frequently than once a week.

The Contractor shall conduct a physical inventory of all controlled and restricted area(s) badges issued to Contractor personnel within 30 calendar days of contract start and on an annual basis thereafter, and shall maintain records of controlled and restricted area badge inventories.

8.26 Combinations

The Contractor shall provide copies of combinations on a separate Standard Form (SF) 700 to authorized personnel. The envelope containing such information shall be marked with the security level, building number, safe or vault number and date of combination change. The Contractor shall change passwords and combinations within 24 hours when Contractor personnel leave the contract, and maintain records of password and combination changes.

8.27 Commander’s Authority

The Government may direct the Contractor in writing to remove any employee from the installation when retention of such employee endangers life, property or security and where such employee violates laws or regulations.

8.28 Transition

The Contractor shall provide a transition plan 14 days after contract award to the CO and Government Program Manager that addresses all actions necessary to ensure a seamless transition.

The Contractor shall coordinate the transition schedule with the incumbent Contractor, NORAD and USNORTHCOM Transition Team, and CO before any transition efforts begin. Identify schedule conflicts to the CO and COR(s).

Transition Activities required, but not limited to:

- ADPE Asset Accountability and transfer of accounts to new Custodians
- Transfer of Safe Combinations
- Transfer of Service Accounts and Administrative Passwords
- COMSEC Account Inventory and transfers
- Provide listing of Security badging requirements by individual
- Determine and Validate backlog of Service Request and Incidents
- Determine and Validate Service Pipeline and Projects
- Provide IT requirements for off-site facility locations

8.29 Purchase Material and Other Direct Costs

All material purchases must be executed on GSA schedules using Harris' deviation 51 authorization letter dated 7 July 2014. Harris will not purchase any open market materials valued above the micro-purchase threshold without written approval from the Contracting Officer. The Contracting Officer will coordinate as necessary with the Lead COR Contractor shall provide an itemized listing of purchased items and title the listing “Government-Furnished Property (GFP).”

8.30 Procurement

The Contractor shall procure all IT hardware, software, equipment, infrastructure, and peripherals required to support this PWS to ensure ITSM priority levels for incident management (break-fix) and request fulfillment (service requests) are achieved. Procurements shall be in compliance with FAR and DFAR. The Contractor shall procure all required IT service assets to support the Contractor produced and Government approved Lifecycle (Technical Refresh) Plan.

8.31 Direct Labor Hour Reporting

The Contractor shall report Direct Labor Hours for this Performance Work Statement. **[CDRL A013].**

The Contractor shall provide the following information annually, no later than 20 days after the end of the government fiscal year. Submission will be provided electronically. The Government has (10) business days to review for correct content and format. If correction is warranted, the contractor has five (5) business days after notice to correct deficiencies and resubmit. Criteria for approval shall be correct content and format.

Contractor will provide Direct Labor Hour report including, but not limited to:

a) Contract Number

b) Performance dates

c) Number of actual direct labor hours used in the performance of the contract requirements for the fiscal year per Labor Category